Thomson Reuters™

Confidentiality rings in English litigation: principles and practice

by Hodge Malek KC, Yash Bheeroo and Devon Airey, 3VB

Status: **Published as on 8 December 2025** | Jurisdiction: **England, Wales**

This document is published by Practical Law and can be found at: **uk.practicallaw.tr.com/w-048-8692**
Request a free trial and demonstration at: **uk.practicallaw.tr.com/about/freetrial**

A practice note that provides guidance on the legal principles and practices governing confidentiality rings in litigation. This note examines the core purpose of a confidentiality ring, also known as a confidentiality club, which is to balance the fundamental principle of open justice against the need to protect genuinely confidential or commercially sensitive information. This note outlines the procedure for applying for a confidentiality ring order and the key factors a court or tribunal will consider, emphasising that such arrangements are an exception and must be necessary and proportionate. It also discusses the different structures a ring may take, including multi-tiered arrangements and highly restrictive "External Eyes Only" tiers, and the critical role of enforceable undertakings. Practical guidance is provided on integrating confidentiality rings into case management and trial preparation, from handling trial bundles to witness preparation and navigating hearings under the Civil Procedure Rules (CPR) where confidential material is involved.

Scope of this document

This practice note considers the legal principles and practices governing confidentiality rings; and provides guidance for parties and practitioners on their creation and use.

Among other matters, the note:

- Examines the principles governing the use of confidentiality rings.
- Outlines the relevant factors a court or tribunal will consider when determining whether to order a confidentiality ring.
- Provides practical guidance on how confidentiality rings are to be integrated into case management and trial preparation.

A confidentiality ring order may be sought alongside other confidentiality measures to protect the use of confidential documents. For example, such documents may be referred to in court only where the court sits in private or is willing to sit in private when considering the document. For guidance on hearings in private see Practice note, Private hearings. For guidance on confidentiality issues arising outside of the litigation context, such as contractual confidentiality clauses, see Practice note, Confidentiality in brief.

What is a confidentiality ring?

A "confidentiality ring" (also referred to as a "confidentiality club") is a court-ordered arrangement that restricts access to documents or information disclosed in litigation to a limited group of named individuals who give enforceable confidentiality undertakings as to their use. These mechanisms are used particularly frequently in competition, procurement, and intellectual property cases, but may arise in other types of cases too.

Confidentiality rings aim to balance the following competing imperatives:

- The fundamental principle of open justice.
- The legitimate interest of the parties to participate meaningfully in the proceedings and have disclosure of all relevant documents that may potentially influence the outcome of the case.
- The need to protect genuinely confidential or commercially sensitive information from wider dissemination or misuse.

Reproduced from Practical Law, with the permission of the publishers. For further information visit uk.practicallaw.thomsonreuters.com or call +44 20 7542 6664. Copyright ©Thomson Reuters 2025. All Rights Reserved.

Relevant legal principles

Principle of open justice

The general rule is that court proceedings are conducted in public, and therefore each party is entitled to unrestricted access to the other's disclosure (subject to certain exceptions). This accords with the "fundamental principle" of open justice (*JC Bamford Excavators Ltd v Manitou UK Ltd and another [2023] EWCA Civ 840 at [71]*).

The principle serves two main purposes:

- To allow public scrutiny of how courts decide cases, so that judges can be held to account for their decisions, and to enable the public to have confidence in the judicial system.
- To promote public understanding of how the justice system works and why decisions are taken – including the issues raised and the evidence relied upon in support of the parties' cases. This is particularly important in modern civil litigation where much of the argument and evidence is reduced into writing, and, therefore, without access to the written material it can be difficult to follow.

(Per Baroness Hale in *Dring v Cape Intermediate Holdings Ltd [2019] UKSC 38 at [42]-[43]* (*Dring*).)

Any restriction on access to disclosed information is therefore a derogation from the principle of open justice (*Libyan Investment Authority v Societe General SA [2015] EWHC 550 (QB) at [20]* (*LIA*); *Aurora Cavallari and others v Mercedes-Benz Group AG and others [2024] EWHC 190 (KB) at [24]* (*Cavallari*)). However, all courts and tribunals retain an inherent jurisdiction to determine what open justice requires to regulate access to documents and information contained within them, a power that exists unless expressly limited by statute. The court's procedural rules do not circumscribe this jurisdiction. The key consideration, therefore, is how the court should exercise that power on a case-by-case basis: see *Dring at [41]*. This is considered further in Creation of confidentiality rings below.

Protection of confidential information

Defining "confidential information" with precision is inherently difficult; documents must be considered within the specific context and facts of each case. While legal authorities provide general guidance against which specific information can be considered, they stop short of providing a comprehensive, fixed set of rules for determining confidentiality. A summary of this position was provided by O'Farrell J in *IBM United Kingdom Ltd v Lzlabs Gmbh and others [2024] EWHC 423 (TCC) at [45]* (*IBM*):

> "45. The legal authorities provide a useful starting point for the test that defines what amounts to confidential information. Confidential information comprises private information that is not in the public domain or accessible readily by persons other than those to whom it has been shown. It may be communicated to selected persons but in circumstances importing an obligation of confidentiality. Confidentiality is a relative and not an absolute concept; in each case, the issue must be considered in context and is fact-sensitive: Bamford v Manitou (above) at [37]-[42]."

See, also, Information must be confidential below.

Balancing the competing legal principles of open justice and confidentiality

While the principle of open justice is fundamental, the courts also recognise the need to protect genuinely confidential information. The Competition Appeal Tribunal (CAT) in *Viasat UK Limited v Office of Communications [2018] CAT 5 at [11]* acknowledged the inherent tension between the prima facie right to open justice and the countervailing necessity of safeguarding legitimate commercial confidences. The CAT concluded that confidentiality rings are a practical mechanism used to "square the circle" between these competing interests.

Accordingly, confidentiality rings are permissible only where justified by the need to protect genuinely confidential or commercially sensitive information. Although their use is becoming more common in modern civil litigation (for example, they are routinely adopted in group litigation actions brought under ss.90 and 90A of FSMA 2000), the courts have consistently observed that such arrangements are "the exception rather than the rule" and the court will only make such an order "if the justice of the case demands" it: see *Porton Capital Technology Funds v 3M UK Holdings Ltd [2010] EWHC 114 (Comm) at [43]* (*Porton Capital*); *Infederation Ltd v Google LLC and others [2020] EWHC 657 (Ch) at [42] (Infederation Ltd)*.

Reproduced from Practical Law, with the permission of the publishers. For further information visit uk.practicallaw.thomsonreuters.com or call +44 20 7542 6664. Copyright ©Thomson Reuters 2025. All Rights Reserved.

It follows that (as per *Viasat*):

- While open justice is fundamental and the "*starting point*", it is not absolute. Each court and tribunal retains an inherent jurisdiction to determine what open justice requires in the specific circumstances of the case.
- Open justice may have to "*give way*" to the need to preserve legitimate commercial confidences of a party to litigation; particularly where that party is defending the proceedings.
- Confidentiality rings are a mechanism by which the courts attempt to balance competing objectives, but they remain the exception rather than the rule.

Creation of confidentiality rings

Court or tribunal's approval required

As confidentiality rings represent a departure from the fundamental principle of open justice, their creation requires approval by the court or tribunal, even where the parties themselves have agreed on the need for (and even the terms of) a confidentiality ring. Ultimately, the court will need to be satisfied that there is a need for such protection and that the creation of a confidentiality ring is appropriate (*Anan Kasei Co Ltd v Neo Chemicals and Oxides (Europe) Ltd [2020] EWHC 2503 (Pat) at [8]* (*Anan Kasei*)). Further, as Roth J said in *Infederation Ltd at [16]*: "... there will always be court scrutiny, and the touchstone of that scrutiny is fairness".

Procedure for applying for a confidentiality ring

Establishing a confidentiality ring requires an application to the court (by Form N244) or request to the relevant tribunal, supported by a witness statement and draft order(s).

While the documents proposed for inclusion in the confidentiality club are typically not provided to the court or tribunal with the application or request, the applicant must provide evidence detailing the nature of the documents (or the section of the document(s)) and explaining why they are confidential and should not be made available for standard inspection. The court or tribunal will not readily accept that the entire contents of a particular document or class of documents are confidential, such that they should not be inspected (*Cavalleri at [29]*).

It is for the party seeking the imposition of a confidentiality ring to make such an application. They will need to justify a departure from the open justice principle by showing that such an order is necessary to prevent a real risk of the documents in question being used for a collateral purpose (*LIA at [21]*; *Porton Capital at [43]*; *Cavalleri at [26-27]*).

See also, Prerequisites for granting a confidentiality ring below, for other matters the court or tribunal must be satisfied of before a confidentiality ring is ordered.

As for the draft order, there is no universal form of confidentiality ring order (often termed a "CRO"). The court or tribunal will determine the appropriateness and terms of such an order based on the specific circumstances of each case. As stated in *Warner-Lambert Co v Glaxo Laboratories Ltd [1975] RPC 354 at [358]*:

> "...having regard to the particular circumstances of the case, bearing in mind that, if a case for disclosure is made out, the applicant should have as full a degree of appropriate disclosure as will be consistent with the adequate protection of any [confidential information] of the respondent".

Factors relevant to the court or tribunal's decision to order a confidentiality ring

The decision whether to order a confidentiality ring involves a balancing exercise between the need for disclosure against the need to preserve confidentiality. Relevant factors the court or tribunal may consider include:

- The degree and severity of the identified risk, and the threat posed by including or excluding particular individuals.
- The desirability of including at least one representative from each party.
- The importance of the confidential information to the case.
- Whether the confidential information requires technical or expert knowledge.
- Practical considerations such as the disruption caused if only part of a legal team can access the information.

(*Oneplus Technology v Mitsubishi [2020] EWCA Civ 1562 at [39]*).

Reproduced from Practical Law, with the permission of the publishers. For further information visit uk.practicallaw.thomsonreuters.com or call +44 20 7542 6664. Copyright ©Thomson Reuters 2025. All Rights Reserved.

The principles relevant to the imposition and terms of a confidentiality ring order have been considered in many authorities, including:

- *Persons Identified in Schedule 1 v Standard Chartered Plc [2025] EWHC 2136 (Ch)* at [117]-[119].
- *Lime Technology Limited v Liverpool City Council [2025] EWHC 1654 (TCC)* at [27]-[34].
- *Magomedov v TPG Group Holdings (SBS) LP [2025] EWHC 1996 (Comm)* at [38]-[43].
- *Weis v Greater Manchester Combined Authority [2025] CAT 27* at [21]-[30].
- *IBM* at [26]-[39].
- *Cavallari* at [20]-[33].

Prerequisites for granting a confidentiality ring

Information must be confidential

Before ordering a confidentiality ring, the court or tribunal must be satisfied that the material in question is genuinely confidential. As to this:

- A duty of confidentiality depends: "not only on the nature of the information and the significance of the information for the [disclosing party], but also on the circumstances of the [receiving party's] acquisition of the information": *Toulson & Phipps on Confidentiality (Sweet & Maxwell, 4th ed, 2020), Chapter 3: Circumstances Importing an Obligation of Confidentiality, paragraph 3-016]* (*Phipps*).
- For information to be confidential, it must have some real value to the party claiming confidentiality. Two conditions are particularly relevant: (i) a reasonable person in the position of the parties would regard it as confidential; and (ii) reasonableness, usage and practices in the relevant sector are consistent with the information being deemed confidential: *Phipps at [4-005]*; *Thomas Marshall Ltd v Guinle [1979] Ch. 227 at p.248B to G*.

However, "confidentiality is not set in stone for all eternity" and may be lost (*Cavallari at [39]*). In particular:

- Information that is "generally accessible" to the public is not confidential: *Attorney-General v Guardian Newspapers (No. 2) [1990] 1 AC 109* at p.282 (*Spycatcher*). However, limited disclosure to certain parties does not necessarily preclude information from being confidential: *Spycatcher at p.260*.
- Commercially sensitive information may lose its confidentiality over time. As per *Phipps at [4-041]*:

  > "Trade secrets, too, may lose their confidentiality by other means than by entering the public domain. In *Thomas Marshall Ltd v Guinle*, Sir Robert Megarry VC suggested, inter alia, that, for information to constitute a trade secret, the party claiming confidentiality must reasonably believe that the release of the information would be injurious to him or of advantage to his rivals or others. A trade secret may cease to have that quality, for example, through changes in the confider's business or through technological advances rendering the trade secret obsolescent."

- Confidentiality may be lost where a party waives privilege or where there is a public interest in revealing information which reveals serious wrongdoing, such that the "inequity exception" applies: see *Al Sadeq v Dechert LLP [2024] EWCA Civ 28 at [52]-[108]*; *Cavalleri at [43]*.

A confidentiality ring will therefore only protect information that remains confidential. Material which cannot be deemed confidential, or has lost that status, will not justify the creation or continuation of a confidentiality ring.

The confidentiality ring must be necessary and proportionate

Even where the information is confidential, a confidentiality ring and its terms must be necessary and proportionate. As Roth J held in *Infederation Ltd at [42]*:

> "... the important points to emerge from the authorities are that: (i) such arrangements are exceptional; (ii) they must be limited to the narrowest extent possible; and (iii) they require careful scrutiny by the court to ensure that there is no resulting unfairness."

Accordingly, the court will examine both: (i) whether a confidentiality ring is genuinely required to protect the information, and (ii) whether the terms of the proposed ring are proportionate to that need. As per the Supreme Court in *Al Rawi v Security Service [2011] UKSC 34 at [11]*: "The question is not one of convenience, but of necessity."

The non-exhaustive factors that are relevant to this assessment may include:

- The nature and sensitivity of the information.
- Whether there is a credible risk (whether deliberate or inadvertent) of collateral use or

Reproduced from Practical Law, with the permission of the publishers. For further information visit uk.practicallaw.thomsonreuters.com or call +44 20 7542 6664. Copyright ©Thomson Reuters 2025. All Rights Reserved.

that information could be misused or cause commercial damage if disclosed more widely.

- Whether the scope of the ring, number of members, and duration of restrictions are no greater than necessary to address the risk. Arrangements where parties themselves are wholly excluded from access are exceptionally rare. The court will also consider the disruption that may be caused if only part of a legal team or no party representative can access the material.
- Whether the ring places one party at a material disadvantage in understanding or responding to the case. The arrangements must not unfairly hamper a party's ability to participate in the litigation or instruct their legal representatives.
- The stage of the proceedings.
- Whether mitigation by less restrictive means (such as, redaction, summarising the essential points without disclosing the full detail (otherwise known as "gisting") or staged inspection) are more appropriate to minimise the departure from the open justice principle.

Pre-existing protections are not sufficient (CPR 31.22)

The Civil Procedural Rules already provide a mechanism to control and restrict the use of documents disclosed in litigation. Under CPR 31.22, a party who receives a document through disclosure must only use that document for the purpose of the proceedings in which it has been disclosed, except where one of the following applies:

- The document has been read to or by the court, or referred to, at a hearing which has been held in public (CPR 31.22(1)(a)).
- The court gives permission (CPR 31.22(1)(b)).
- The party who disclosed the document and the person to whom the document belongs agree (CPR 31.22(1)(c)).

Further, pursuant to CPR 31.22(2), the court may make an order restricting or prohibiting the use of a document which has been disclosed, even where the document has been read to or by the court, or referred to, at a hearing which has been held in public.

For more on disclosure under CPR 31, see Practice note, Disclosure: who must give disclosure and what is the disclosure obligation?: Can documents provided on disclosure be used outside the proceedings?.

Given that CPR 31.22 already limits collateral use of disclosed documents, the courts will only order a confidentiality ring where there is credible evidence of a real risk that the existing protections would be insufficient. As noted by Cockerill J (as she then was) in *Cavallari at [24]*, in most cases and for most documents, the collateral undertaking under CPR 31.22 will provide sufficient protection.

That said, the protection offered by CPR 31.22 was found to be insufficient in *IBM* - a dispute concerning the alleged unlawful use of IBM's confidential mainframe software. O'Farrell J noted at [35] that while in most cases CPR 31.22 will provide sufficient protection against the misuse of documents,

> "...such orders can be difficult to police and, once confidentiality has been breached, the information is in the public domain. The parties agree in this case that, on both sides, there is confidential information that is so commercially sensitive that it requires additional protection, through restricted access to the documents."

Composition and structure of confidentiality rings

The composition and structure of a confidentiality ring depend on the circumstances of each case: see *Infederation Ltd at [24]*.

The structure and composition may be varied over time; for example, to admit additional members to the confidentiality ring or after determining whether specific documents really are confidential (see Varying or amending terms and Review of confidentiality designations before trial).

Determining membership

When deciding whether an individual should be admitted to a confidentiality ring, the court or tribunal considers their role, responsibilities, jurisdiction in which they are based, and the risks posed by their access to the material. Paragraph 40 of Appendix H of the Technology and Construction Court (TCC) Guide provides guidance on the relevant factors to be considered, including:

- The individual's function and involvement in the litigation.
- The likelihood and gravity of harm that could arise from disclosure to them.
- Whether the risk can be mitigated through undertakings or conditions of access.

Reproduced from Practical Law, with the permission of the publishers. For further information visit uk.practicallaw.thomsonreuters.com or call +44 20 7542 6664. Copyright ©Thomson Reuters 2025. All Rights Reserved.

- The impact that exclusion or inclusion would have on that person's ability to participate effectively in the case.

Such guidance was also considered in *Camelot UK Lotteries Limited v The Gambling Commission [2022] EWHC 1102 (TCC) at [30]*.

There may be good reasons why only professionals, such as lawyers and experts, should be admitted into the confidentiality ring. For example, where the parties are competitors and the confidential information is such that a party may gain a competitive advantage or they may be able to reduce competition on the market by using information disclosed within proceedings.

Where a party contends a person should be admitted to a ring, the court or tribunal will ordinarily defer to that party's judgment: "*the court should be slow to second guess that contention. It is, after all, a basic right of every party to conduct litigation as he, she or it sees fit...*" (*Anan Kasei at [16]* (as cited in *Lime Technology Limited v Liverpool City Council [2025] EWHC 1654 (TCC) at [30]*)).

However, a court or tribunal will not automatically grant access to a person where there is a concern as to the suitability or necessity of that person becoming a member of the ring. In such cases, the court or tribunal may grant access on a limited basis, subject to additional protections, or only to specific documents in the ring.

Such an issue was considered by the Competition Appeal Tribunal in *Weis v Greater Manchester Combined Authority [2025] CAT 27*, discussed in Legal update, Ruling on admission to a confidentiality ring in application for review under Subsidy Control Act 2022 of alleged subsidy by Greater Manchester Combined Authority (CAT). The issue in *Weis* was whether the appellant's son, J, should be granted access to commercially sensitive financial information belonging to a direct competitor, R. This situation arose because the appellant needed a client representative to review key documents to provide instructions to his legal team. The CAT admitted J to the confidentiality ring, notwithstanding the CAT's acknowledgement (*at [37] and [54]*) that granting a competitor direct access to such sensitive information would normally be refused. To mitigate the risks associated with allowing J access to such confidential information, the CAT imposed two protections (*at [59]-[60]*):

- That the appellant and his son, J, provide appropriate undertakings that they would not use the disclosed material for any other purpose and would not disclose it otherwise than to their own legal team in connection with the proceedings.
- That the information would only be disclosed to J at a meeting with the appellant's solicitors. If a witness statement was needed from J, it would be taken at the solicitors' offices. J would not be allowed to remove the statement from those premises unless it was a redacted version, which omitted the relevant confidential information.

Another example of the CAT's consideration of whether to admit a particular individual into a confidential ring, and the factors it took into consideration, can be found in *Viasat UK Ltd v Office of Communications [2018] CAT 14 at [9]-[23]*.

Structure of confidentiality rings

Confidentiality rings are often structured in tiers with membership reflecting gradations of sensitivity.

Single-tier rings

In general, confidentiality rings operate at two levels, even where the confidentiality ring is a "single ring". As the CAT held in *Boyle v Govia Thameslink Railway Limited and others [2024] CAT 26 at [2]-[3]*:

> "[2]... An order – here the Confidentiality Ring Order – establishes the ring. Certain individuals are then admissible to the ring, and usually are identified in an annex to the order, which is "ambulatory", in that it varies according as to who is admitted and who leaves the ring. This is what we term the "first level".
>
> [3] The price of admission to the ring on the part of the individual is the giving of undertakings directly to the Tribunal. This is what we term the "second level", a personal undertaking given by each individual admitted to the ring. Only upon the giving of those undertakings are such individuals permitted to access the information that is placed inside the confidentiality ring."

Two-tier or multi-tier rings

Two-tier (or multi-tier) rings are increasingly common in complex litigation, especially in intellectual property, competition and procurement cases. For example, in *InterDigital Technology Co v OnePlus Technology*, the confidentiality regime comprised an "External Eyes Only" tier (restricted to external lawyers and experts) and a "Highly Confidential" (HCONF) tier (permitting access to named individuals within the party, such as in-house counsel).

The two-tiers may sometimes be described as being the "inner confidentiality ring" and the "outer

Reproduced from Practical Law, with the permission of the publishers. For further information visit uk.practicallaw.thomsonreuters.com or call +44 20 7542 6664. Copyright ©Thomson Reuters 2025. All Rights Reserved.

confidentiality ring". The inner confidentiality ring is typically more restrictive and admission to this tier of the confidentiality ring may, for example, be limited to external legal representatives only.

The TCC Guide (Appendix H, paragraphs 41-42) sets out circumstances in which a two-tier structure may be appropriate:

- Two-tier rings are typically used where it is necessary to gradate the level of access to confidential information. For example, employee representatives may be admitted to a confidentiality ring on different terms from external legal representatives whereby the employee representatives have access to some, but not all, of the material disclosed into the ring.
- Alternatively, the external representatives of a party in the first tier may apply for an employee representative in the second tier to have access to a particular document or documents, whether in open form or partly redacted. One way of dealing with this is for notice to be given to any person affected by the proposed disclosure, identifying the document, the form in which its disclosure to members of the second tier is sought, and the reasons why disclosure to the second tier is sought, and for the person affected to consent or object within a fixed time.
- Two tier rings necessarily introduce additional cost and complexity and will therefore need to be justified in the circumstances.

See also *Bugsby Property LLC v LGIM Commercial Lending Limited and ors [2021] EWHC 1054 (Comm) at [83]*, discussed in Legal update, Non-party disclosure ordered in Disclosure Pilot Scheme case, subject to tiered confidentiality ring (Commercial Court).

External Eyes Only

"External Eyes Only" is the most restrictive tier. It typically excludes all client representatives of a party from viewing the information, limiting access to external lawyers and (sometimes) experts. Because it prevents a party from seeing documents that may be material to its own case, the courts and tribunal regard it as an exceptional measure.

It has been suggested that restricting document access to "external eyes only" must be kept to exceptional circumstances because it allows one party to unilaterally deny the restricted party access to any documents they choose, shifting the burden onto the restricted party to seek access. Such blanket exclusions have been considered to violate the right to a fair hearing under Article 6 of the European Convention on Human Rights, principles of natural justice, and lawyers' professional obligations to share all relevant information with their clients when acting on their behalf. (See *TQ Delta v Zyxel [2018] EWHC 1515 (Ch) at [21]ff*, discussed in Legal update, "External eyes only" confidentiality should be ordered only in exceptional cases (Patents Court).)

Given the exceptional nature of an "external eyes only" order, the disclosing party must be able to justify the continuation of the restrictions for each of the affected documents or classes of documents (*JSC Commercial Bank Privatbank v Kolomoisky [2021] EWHC 1910 (Ch) at [44]*).

Staged disclosure of confidential information

In *OnePlus Technology (Shenzhen) Co. Ltd and others v Mitsubishi Electric Corporation and another [2020] EWCA Civ 1562* (discussed in Legal update, Guidance on disclosure of confidential information in FRAND case (Court of Appeal)), Floyd LJ disagreed that an approach where prima facie highly confidential documents are first disclosed on an external eyes-only basis is wrong in principle. The authorities establish that staged or progressive disclosure of confidential information is permissible. Floyd LJ considered an alternative approach, where courts would individually examine each document before granting "attorneys' eyes only" (AEO) designation, which would require limited initial disclosure to the opposing party followed by a court determination based on submissions from both sides. However, Floyd LJ concluded that there is no substantive difference between this approach and allowing the disclosing party to initially designate documents as AEO, provided the receiving party can challenge that designation and the disclosing party does not abuse the process (*judgment at [36]*).

An example of a staged approach to confidentiality is *LLC EuroChem North-West-2 v Societe Generale SA [2025] EWHC 1938 (Comm)*, where 55 documents were initially placed within a confidentiality ring on a provisional basis, pending review of the confidentiality designations and the proposed ring provisions by the court.

Counsel only

In exceptional cases involving public interest immunity or national security, access may be restricted to counsel only. This approach was adopted in *R (on the application of Hoareau) v Secretary of State for Foreign and Commonwealth Affairs [2018] EWHC 3825 (Admin) at [39]-[44]*.

Reproduced from Practical Law, with the permission of the publishers. For further information visit uk.practicallaw.thomsonreuters.com or call +44 20 7542 6664. Copyright ©Thomson Reuters 2025. All Rights Reserved.

Non-party participation

Although confidentiality rings primarily concern parties to proceedings, the court or tribunal retains discretion to include non-parties where their participation is necessary; for example, an expert witness, a third-party data provider, or an affected contractual counterparty. Admission of a non-party into a confidentiality ring is subject to the same scrutiny and undertakings as for party representatives. See, for example, *Infederation Ltd* where the claimant's application to admit its independent expert, a search engine optimisation consultant, was granted.

Undertakings

Confidential information is only made available to members of a confidentiality ring once they have provided formal undertakings to the court or tribunal. These undertakings are enforceable and are a critical safeguard against the misuse of the information disclosed within the ring. Typical undertakings include commitments to:

- Use the information solely for the purposes of the relevant proceedings.
- Refrain from disclosing the information to anyone outside the confidentiality ring.
- Comply with specific handling requirements, such as restrictions on copying, storage, where the documents may be viewed and communication.
- Return, destroy or render inaccessible all confidential material at the conclusion of the proceedings.

Depending on the subject matter and risk of misuse, the court or tribunal may require additional undertakings to address particular concerns. This is especially likely in competition, procurement, or regulatory cases, where the disclosure of sensitive commercial information could affect market conduct. Examples of additional undertakings include commitments that:

- A recipient will not participate in or advise on any re-procurement process relating to the contract that is the subject of the litigation.
- The recipient will not take part in tenders or projects involving similar contracts within a defined period or area.
- The recipient will refrain from advising on matters or markets for a fixed duration.
- The confidential information will only be communicated to a party, subject to specific restrictions, including restrictions on quoting from or summarising the contents of the confidential information.

Breach of undertaking may constitute contempt of court

As the undertakings are given directly to the court or tribunal, their breach may constitute contempt of court. This mechanism provides an additional layer of protection, ensuring that members of the ring fully understand the seriousness of their obligations and the potential consequences of non-compliance.

For more information on contempt of court generally, see Practice note, Contempt of court: overview.

Jurisdictional limitations

However, effective enforcement is likely to be more challenging when dealing with persons based outside the jurisdiction. While making the inclusion of foreign individuals conditional on the provision of suitable undertakings may offer a partial solution, the court or tribunal may still lack the practical means to penalise a non-compliant individual abroad for breaching disclosure restrictions. These jurisdictional limitations may therefore militate against including individuals based outside of the jurisdiction in the confidentiality club, particularly where their inclusion poses a demonstrable risk of prejudice to the interests of the party which obtained the confidentiality ring.

Varying or amending terms

The terms of a confidentiality ring may require adjustment as proceedings develop; for example, to add or remove members, modify document designations, or alter the structure of the ring.

Where a change is required, parties typically proceed by way of written application or consent order referencing the original CRO. The application should identify the specific amendments sought and explain why the variation is necessary.

Many CROs include a procedural mechanism for future variations. Such clauses provide clarity and efficiency while maintaining judicial oversight. These mechanisms typically include:

- A requirement that any party wishing to vary membership must give written notice to the other parties.
- Specification of what the notice must contain (for example, the identity and role of the proposed individual and the reasons for their inclusion).

Reproduced from Practical Law, with the permission of the publishers. For further information visit uk.practicallaw.thomsonreuters.com or call +44 20 7542 6664. Copyright ©Thomson Reuters 2025. All Rights Reserved.

- A defined period for other parties to consent or object.
- A process for referring any objections to the court or tribunal for determination.
- Miscellaneous provisions, including that the party seeking to vary the terms of membership must provide an updated annex listing all members of the ring.

As confidentiality rings are exceptional, the court or tribunal will expect parties to keep their necessity under review. If the confidential status of documents changes, the ring may be varied or discharged accordingly. (See, also, Review of confidentiality designations before trial.)

Practical considerations after a confidentiality ring has been ordered

While the legal principles governing confidentiality rings are well established, their practical operation raises several procedural issues. This section outlines key considerations for parties and practitioners in handling confidential material when preparing for and at trial.

Before trial

Once a confidentiality ring has been ordered, parties must ensure that its terms are fully integrated into their case management and trial preparation. This may include, but is not limited to, the following suggestions.

Managing confidential material and coordination between legal teams

The following precautions should be taken to minimise the risk of inadvertent disclosure of protected documents:

- Parties should maintain a clear record of which documents are designated as being within the confidentiality ring and who is permitted access to them. This record should be reviewed regularly. This will usually be recorded in a "Confidentiality Ring Register", which each party is expected to maintain and update throughout the proceedings.
- Where a two-tier or multi-tier structure exists, each document must be clearly designated as belonging to a specific tier (for example, "External Eyes Only" or "Inner Confidentiality Ring Only").
- In cases where only part of a party's legal team (such as external counsel and selected solicitors) is admitted to the ring, the team must establish clear internal communication protocols. For example:
  - confidential material should not be discussed with non-ring members unless expressly permitted by the order;
  - draft submissions, skeleton arguments, and witness statements should be checked for inadvertent inclusion of confidential content;
  - internal correspondence and file systems should separate confidential ring material from other case documents.
- Where possible, firms should use secure electronic repositories or document management systems with controlled access, audit trails, and encryption to manage these restrictions effectively.

Trial bundles and document handling

Consider the following precautions to protect confidential documents in trial bundles:

- Separate confidential bundles should be prepared for confidential materials.
- These must be clearly marked (for example, "Confidentiality Ring – Not for Wider Circulation") and handled in accordance with the order's terms.
- Where practical, redacted versions should be prepared for open use, enabling open hearings to proceed where possible.
- It often assists to create a confidential annex or index specifying which bundles or sections are confidential for the court's or tribunal's reference.
- Confidential bundles should be transmitted and stored securely.
- If the trial will be partly heard in private, the parties should identify and agree in advance which materials are likely to require private handling so that the timetable and logistics can, where necessary, accommodate this division.
- Parties may also consider whether the documents could be read by the court and the parties without being openly read out or referred to in court, although this is likely to be more appropriate where the documents to be referred to are limited in nature.

Review of confidentiality designations before trial

The court may review the provisions of any CRO at different stages of the litigation. This includes assessing the necessity for the restrictions to

Reproduced from Practical Law, with the permission of the publishers. For further information visit uk.practicallaw.thomsonreuters.com or call +44 20 7542 6664. Copyright ©Thomson Reuters 2025. All Rights Reserved.

persist through to trial or determining if substitute protective measures should be implemented. This review will generally occur at the Pre-Trial Review (PTR), although the court may list another case management hearing for the purposes of reviewing whether the restrictions should be maintained.

Courts and tribunals increasingly expect parties to conduct such reviews proactively.

Witness preparation and expert evidence

Consider the following when dealing with witnesses of fact or expert witnesses:

- Where a witness is a member of the ring, they may be shown the relevant materials subject to their undertakings.
- If a witness is not a ring member, they cannot be provided with confidential documents unless granted permission. Possible approaches include:
  - preparing redacted versions of documents, where necessary, for the witness; or
  - providing summaries that omit the confidential content insofar as this is not prohibited by the terms of the CRO or the relevant undertakings.
- Experts are often admitted to confidentiality rings, especially in cases involving technical, scientific or economic evidence. The instructing party must ensure that the expert understands the undertakings and complies with them in full. Instructions to the expert should clearly state:
  - the existence and terms of the CRO;
  - the limits on disclosure of information to others within their firm or organisation; and
  - the procedures for storing, discussing and disposing of confidential materials after the report is completed.
- It is good practice to ensure experts confirm in writing that they have read and understood their obligations under the CRO.

At hearings and trial

The use of a confidentiality ring at trial may necessitate an application for the court or tribunal to sit in private, or partly in private, to prevent the disclosure of confidential material during oral evidence or submissions. The starting point, however, is that hearings are to be held in public: CPR 39.2(1).

The requirements for such an application fall outside the scope of this note, but they closely mirror those that apply to the creation of a confidentiality ring. In particular:

- The rule that hearings and judgments are public reflects the fundamental principle of open justice, as reaffirmed in *Al Rawi v Security Service [2011] UKSC 34* and *Dring v Cape Intermediate Holdings Ltd [2019] UKSC 38*.
- Any derogation must be necessary and proportionate. CPR 39.2(3)(c) provides that a hearing, or any part of it, must be held in private if, and only to the extent that, the court is satisfied "it involves confidential information… and publicity would damage that confidentiality". The burden rests on the party seeking such an order to show that it is necessary to secure the proper administration of justice.
- Applications under CPR 39.2(3)(c) require clear and cogent evidence that there is a real risk of misuse of confidential information if referred to in open court.
- As with CROs, any limitation on publicity must go no further than required. The court may, for example, sit in private only temporarily or redact specific passages from documents, rather than excluding the public altogether (see *Ambrosiadou v Coward [2011] EWCA Civ 409 at [50]-[51]*). Often, the need to keep going in and out of private when confidential documents are referred to can be avoided by counsel not reading from such documents, but instead asking the court or tribunal to read the relevant passages to itself.

Legal solutions from Thomson Reuters
Thomson Reuters is the world's leading source of news and information for professional markets. Our customers rely on us to deliver the intelligence, technology and expertise they need to find trusted answers. The business has operated in more than 100 countries for more than 100 years. For more information, visit www.thomsonreuters.com

Thomson Reuters™