



INSPIRE CONTRACT SERVICES LIMITED

COMPETITION LAW HANDBOOK

CONTENT SUMMARY

COMPETITION LAW POLICY

- | | |
|------------------|---|
| Section 1 | Introduction & Commitment |
| Section 2 | Compliance Procedures <ul style="list-style-type: none">2.1 Are your actions compliant?2.2 Reporting suspected infringements2.3 Dawn Raids |
| Section 3 | The Law <ul style="list-style-type: none">3.1 Main provisions3.2 Investigatory powers3.3 Consequences |

QUICK COMPLIANCE

1. Compliance in Tenders
2. Information Sharing
3. Competitor Contact at Trade Associations and Industry Events
4. Key Dos and Don'ts for New Employees

DAWN RAIDS ROLE BY ROLE GUIDANCE

Section 1 – Policy

Introduction

Competition law aims to safeguard free and fair competition between companies for the benefit of consumers. Fair competition encourages innovation, delivers high-quality goods and services at fair prices and enhances consumer choice. Accordingly, competition laws around the world are designed to deter breaches of competition law by harshly punishing companies and individuals involved.

Inspire Contract Services Limited has a reputation for excellent client service, and we believe in doing the right thing for our customers. We are committed to competing ethically and fairly for all contracts and want to ensure that our practices across the business reflect that commitment. Considering the renewed focus of the Competition and Markets Authority on the roofing industry, it is particularly important that our practices reflect best practice and ensure compliance with competition law. This policy enshrines our values into formal policy and outlines Inspire's overarching commitment to comply with competition law at all levels of the organisation.

Employees have a duty to conduct their business dealings in line with the Policy. Any instance of acting in a way that infringes competition law will be taken very seriously and may lead to disciplinary action. The Policy's objective is to ensure compliance with the law and to deal effectively with any competition law claims or investigations by competition authorities or third parties. In the event that you have any questions regarding this policy or competition compliance in general, please do not hesitate to contact Gary Slawson.

Thank you for helping Inspire compete fairly.

Policy Statement

- 1.1 The Company is committed to comply with all relevant competition law legislation.
- 1.2 The board of directors is responsible for ensuring that compliance with competition law permeates the organisation.
- 1.3 All employees:
 - 1.3.1 shall conduct their business dealings in line with this Policy;
 - 1.3.2 shall act in such a way as to avoid any breach of competition law;
 - 1.3.3 shall familiarise themselves with the basic provisions of competition law;
 - 1.3.4 shall consider the competition law aspects of their work and if appropriate take relevant advice before committing to a course of action, making a decision or reaching an agreement; and
 - 1.3.5 must attend training sessions, partake in online compliance programmes and read associated best practice updates as directed.
- 1.4 Disciplinary action may be taken against any Relevant Employee who intentionally or negligently infringes competition law or any aspect of this Policy.
- 1.5 Relevant Employees who suspect that their business dealings may infringe competition law shall immediately notify Gary Slawson via the communication channels specified in *Section 2.2 – Reporting suspected infringements*.

Section 2 – Procedures

This section establishes a framework to enable employees to assess whether a particular interaction complies with competition law, the process to clarify the position when there is any doubt and report activities that they suspect may infringe competition law.

2.1 Are your actions compliant?

1. Refer to *the Quick Compliance guides*
2. Refer to any relevant competition law training you may have received.
3. Consult your line manager – it may be necessary to take external legal advice from our solicitors.

2.2 Reporting suspected infringements

It is essential that any employee that is aware of, or potentially involved in, activity that may infringe competition law can report the matter. If an employee is involved in an infringement of competition law, directly or indirectly, Gary Slawson must be informed immediately. The Senior Leadership Team will assess the nature of the issue and a judgement will be made on whether to obtain external legal advice.

The Company also operates a Whistleblowing Policy, which allows employees to raise any matter which concerns them in the knowledge that this will be taken seriously, treated as confidential and that no action will be taken against them – a copy of this policy is available on the company server.

2.3 Dawn Raids

In the event of an investigation of suspected anti-competitive practices, it is usual for a company to co-operate fully with the authorities whilst taking appropriate steps to protect its legal rights. Such an investigation could include an unannounced inspection of company premises, otherwise known as a “dawn raid”. If Inspire is subject to a dawn raid, please follow the role-by-role guidance included within this handbook.

Section 3 – The Law

Competition law is designed to promote economic growth through genuine survival of the fittest and encouraging a lawfully entrepreneurial environment in which to trade.

Competition law applies to all levels of the supply chain, and the Company must, therefore, ensure that our relationships with customers, suppliers and competitors always comply with the law.

3.1 Main Provisions

The Competition Act 1998 (“**the Act**”) prohibits anti-competitive behaviour within the UK. The Act is applied and enforced by the Competition and Markets Authority (the “**CMA**”).

The Act contains two key prohibitions:

- a prohibition of anti-competitive agreements between businesses and decisions by associations of businesses; and
- a prohibition of abuse of market power by a business having a dominant position.

Anti-Competitive Agreements and Concerted Practices

Agreements or concerted practices between businesses which have the object or effect of preventing, restricting or distorting competition in the UK are prohibited.

An agreement may be formal (legally binding contracts) or informal (a gentleman’s agreement, a handshake agreement, or a mutual understanding). This means that an agreement could be entered into by a simple whatsapp conversation, or during a conversation in a pub or on the golf course. An agreement also doesn’t need to be implemented to be caught by competition law.

A concerted practice falls short of an agreement and can occur if there is direct or indirect contact between businesses which leads to some level of co-ordination between them. For example, sharing details of bidding information, even though there is no agreement to use the information to enter cover prices, would nevertheless allow the businesses to co-ordinate their bidding behaviour. Concerted practices can also arise from informal conversations and, in particular, from meetings and discussions at trade associations and industry events.

These are some types of anti-competitive agreements that are *presumed* by the CMA to be anti-competitive:

- **Price fixing** - agreements to fix prices can occur between competitors or between a supplier and a retailer. “Price” means **any part of the price** and, therefore, includes margins, discounts, commissions, rebates. Co-ordinating the timing of pricing changes may also amount to price fixing.
- **Market sharing** - this is where competitors agree to divide up markets by location or by customer groups. For example, a business agrees with a competitor that it will supply products in the north of England and the competitor will only supply in the south.
- **Bid rigging** - this is where a company agrees with a competitor that the company will not tender for a certain contract or alternatively, that it will tender for that contract at an artificially high price in exchange for the competitor doing the same on another contract.

Any agreement that has the object or effect of restricting or distorting competition in the UK is caught by competition law.

Abuse of a Dominant Position

The Competition Act also prohibits abuse of a dominant market position.

There is no clear rule on when a company will be considered dominant. As a rule of thumb, a company that has a market share of less than 40% is unlikely to be dominant, unless its competitors have very small market shares. A company with a market share of between 40% and 50% may be dominant; if a company has a market share of more than 50% it is presumed to be dominant.

It is not unlawful for a business to be dominant in a particular market. A dominant firm is, however, under a special responsibility not to abuse its position in the market. Examples of what would constitute an abuse of a dominant position include:

- imposing excessive prices for products or services;
- providing products or services at below cost (predatory pricing);
- unjustifiably refusing to supply (whether price- or customer-related);
- charging different prices to equivalent customers, with no objective justification (discriminatory pricing);
- forcing customers to buy unrelated services (tying arrangements).

3.2 Investigatory Powers

The CMA have far reaching powers of investigation when they have reasonable grounds for suspecting that there has been a breach of competition law.

The CMA can instigate an investigation based on a tip-off from one of our competitors, our customers or anyone else in the supply chain. They can also begin an investigation if they suspect foul-play in our marketplace. Where the CMA suspect an infringement by a company, they are able to:

- send a letter to a company asking for specified documents or specified information to be produced. Documents that can be requested include memos, minutes of meetings, business and personal diaries, emails (including personal ones), letters and faxes; and
- enter and search business premises/vehicles and domestic premises if these are used by employees and documents relating to the business are kept there - this is known as a “**dawn raid**”.

During a dawn raid CMA officials may:

- use reasonable force to obtain entry to premises;
- examine, and take copies of, the company's books and other business records;
- ask for oral explanations on-the-spot as to location and content of documents;
- seize original documents; and
- require any information which is held in electronic version and is accessible from the premises to be produced in a form in which it can be taken away and which is visible and legible.

The CMA have additional powers to investigate individuals they suspect of being involved in price fixing, market sharing or bid rigging conduct. These powers include being able to conduct directed surveillance and covert human surveillance on any individuals they suspect of being involved in such activities.

3.3 Consequences

Breach of competition law can result in severe consequences for individuals, including Inspire's directors, and for the Company itself. It is therefore in the interests of all employees to ensure that the Company is compliant with the law.

The consequences of breaching competition can include:

- Time-consuming and expensive investigations that may prove a distraction in fulfilling our contracts;
- A fine of up to 10% of group turnover;
- Debarment from public procurement exercises, stopping us from bidding in government tenders;
- Damage to the Company's good name and reputation and in particular, our credibility with customers;
- The possibility of imprisonment or fines for individuals involved in anti-competitive behaviour;
- Disqualification from acting as a director for up to 15 years; and
- Potential actions for compensation from affected third parties.

In short, no amount of gain, either for the Company or the individual, are worth the risks of breaching competition law.

Quick Compliance: Compliance in Tenders

Bid rigging is type of market sharing where competing businesses secretly cooperate to manipulate the outcome of a tender or bidding process, rather than competing fairly. It is a serious breach of competition law, and carries a significant risk of fines, director disqualification and debarment from public procurement exercises. When carrying out a procurement exercise, customers are seeking to secure the best deal in a competitive process. Bid rigging tricks the customer into thinking they have get the lowest price possible whereas, they could have paid less if they had received all genuine quotes. Inspire is strictly against bid rigging and does not tolerate bid rigging in any form.

Common bid-rigging practices include

- Cover pricing – competitors submit deliberately high or non-competitive bids so a chosen party wins
- Bid suppression – one or more competitors agree not to bid
- Bid rotation – firms take turns winning contracts
- Subcontracting arrangements – the “losing” bidder is rewarded with work from the winner

In order to minimise the risk of any bid rigging, follow the following dos and don'ts:

Do	Don't
DO make independent decisions on whether or not you want to compete in a particular tender.	DO NOT ask competitors if they are intending to participate in a particular tender. Knowing whether or not a competitor is intending to submit a bid may influence your own pricing and so is considered commercially sensitive.
DO make unilateral decisions on pricing, and compete honestly in tenders.	DO NOT ask competitors how they are pricing a job – even if it is not a job that you wish to win but feel obliged to submit a bid for. Every tender response must be created independently and without the input of competitors.
DO tell a member of the SLT if a competitor approaches you with a proposal to collaborate (or partner) in relation to a given job or customer. It may well be legitimate to do this, but will require careful structuring.	DO NOT discuss the price or bidding strategy with competitors or any other parties whilst on site visits .
DO act independently in the market deciding unilaterally the price at which you quote customers, surveyors or third parties, and reject any attempt by a competitor to influence your pricing decisions.	DO NOT offer “friendly names” to a surveyor or technical advisor if asked, parties must genuinely compete on each tender.
DO decide unilaterally, and in compliance with our practice the prices and terms at which you submit tender responses for work.	DO NOT ask a surveyor for information on the pricing of other bidders.
DO consider whether you want to win a job before submitting a tender, including whether you have capacity to service the work at the time.	DO NOT accept any financial benefit or kickback for not bidding on a project, or bidding at a certain level.

Quick Compliance: Information Sharing

Receiving and sharing information is a normal part of our work and helps us compete effectively within the market. However, we should take care when receiving or sharing information that we are doing so in compliance with competition law.

This quick compliance guide covers what you need to remember about:

- Information that you should not exchange with competitors, distributors or suppliers;
- What you should do if you are concerned about any information exchange that has taken place; and
- Tips for dealing with competitors.

What Information can I share?

Sensitive

- × Customer lists and information
- × Trading terms
- × Volume forecasts
- × Business strategy
- × Future pricing information
- × Future product specifications
- × Investment and production costs

Careful

- ≈ Historic data
- ≈ Best practice
- ≈ Market trends

Safe to exchange

- ✓ Practical issues and standards
- ✓ Legal developments

What is classed as an exchange?

Exchanging information by any means or in any format may be caught by competition law. This includes written and verbal communication across any platform, including whatsapp communications whether on work or personal devices. An exchange does not have to be reciprocal - even a one-way flow of information may be caught, and has resulted in significant fines for other business previously.

Information can be exchanged through direct contact with competitors, or indirectly through third parties. You should be careful in dealing with any third parties who may pass information on to your competitors, including common suppliers, surveyors, customers or other industry bodies.

Information may also be considered to have been an unlawful exchange even if you were simply party to a discussion where strategic information was shared by a competitor as part of a wider discussion with others at which you were present, for example during a trade association meeting. If a company receives strategic data from a competitor, **it will be presumed to have accepted** the information and **adapted its market conduct** unless it responds with a clear statement that it does not want to receive such data

What should I do if I think there has been an unlawful disclosure of competitively sensitive information?

If you think you have disclosed competitively sensitive information to a competitor or third party, it is important that you do not try to hide your mistake. In the first instance you should contact Gary Slawson or any other Inspire Director and inform them of the details of the disclosure including:

1. What information was disclosed;
2. Who the information was disclosed to;
3. How and when the information was disclosed; and
4. The response of the individual involved in the disclosure.

The senior leadership team will then tell you what actions you need to take. This may include contacting the individual to whom the information was disclosed and asking that they destroy the information (if possible), and/or obtaining advice from external legal advisors.

What should I do if I receive competitively sensitive information from a competitor or third party?

If you receive competitively sensitive information pertaining to a competitor from a competitor or third party, you must report it immediately to Gary Slawson or any other Inspire Director. When reporting the disclosure, do not send the information on to Gary or the directors in the first instance, instead provide a brief summary of the facts, including:

1. A high-level description of the information that was disclosed (e.g. information relating to pricing for a tender);
2. Who sent or otherwise disclosed the information to you;
3. How and when the information was disclosed; and
4. Any initial actions taken by you.

The senior leadership team will then tell you how to respond. This may include contacting the individual who disclosed the information and informing them that you do not wish to receive this kind of information and have ensured its deletion, requesting that this information is not shared with you again, and/or obtaining advice from external legal advisors.

What Penalties are there for unlawful information exchange?

Breaching competition law can lead to serious consequences for yourself and the company:

- individuals who are found guilty of breaching competition law can be fined or even imprisoned. Directors who breach competition law may be disqualified from acting as a company director.
- Companies that breach competition law can be fined up to 10% of group worldwide turnover and prohibited from bidding in public procurements.
- Investigations by competition authorities can be lengthy, costly, disruptive to business and generate adverse publicity.
- Third parties that suffer loss or damage as a result of a company's breach of competition law may also bring claims against the company.

A customer has sent me another party's quote for a job and asked if I can match it – is this information sharing?

It is common practice for customers to obtain a number of quotes and use them as tools to negotiate with suppliers, and provided this is the customers intention, this is not an anticompetitive agreement. However, if the customer is being used to exchange commercially sensitive information between the parties, this is problematic. We would recommend that any quotes shared by customers to suppliers and anonymised so as to mitigate risk of price coordination.

Do	Don't
Remember that even a one-way disclosure of commercially sensitive information by a competitor may be considered a breach of competition law.	Do not share any commercially sensitive information with competitors, either directly or indirectly, and whether during a formal or informal meeting or social gathering.
Inform the Senior Management Team as soon as you can if you believe you have been a party to a disclosure of competitively sensitive information	Never assume that it is okay to share information because others are doing so. If you consider there is a legitimate reason for exchanging information with a competitor, you must seek the prior approval of the Senior Management Team .
Speak up if a competitor tries to discuss commercially sensitive information with you or if you are concerned that the discussion is straying into "dangerous waters", irrespective of whether this is verbally or in written communication. Remember: OBJECT – MINUTE – LEAVE – REPORT .	If you receive something concerning from a third party (whether competitor, customer or supplier), do not forward this information to anyone else in the business.
Keep a record of discussions with competitors.	Do not pass one subcontractor's commercially sensitive information to another subcontractor. If you are seeking to ask a subcontractor to meet a quote another subcontractor has provided, anonymise the quote before sending.
Do make unilateral decisions on pricing.	Do not ask a technical advisor to provide information about a competitor's future pricing or other commercially sensitive information relating to competitors.

Quick Compliance: Competitor Contact at Trade Associations and Industry Events

It is important to remember that contact with competitors can occur in a number of different contexts, including trade association meetings, supplier days, corporate entertainment, sports fixtures, group chats, awards dinners, and where a supplier or subcontractor happens also to be a competitor. Contact with competitors is a normal part of industry, but it is important that conversations with competitors do not stray into topics which could pose a competition risk.

Uncertainty between competitors as to what each other is doing (or might do) in the market is one of the key drivers of independent behaviour (and therefore competition). Recent cases and guidance from the competition authorities indicate that they may infer the existence of an anti-competitive “agreement” if one competitor merely receives relevant commercially confidential / sensitive or strategic information from another and can be taken to have acted on it. In other words, there is no requirement for reciprocity in terms of information exchange for an infringement to occur.

When you send or receive information, you should ask yourself the following question:

“Is the information that a person is about to share information which, in the hands of the recipient, could reveal something about the way the person sharing the information might behave in another context (for example in the context of dealings with a prospective customer that both the person sharing the information and the recipient of the information might be interested in supplying)?”.

Trade associations and industry events are a high-risk environment, whilst they can be a useful forum to discuss issues facing the industry, they can also present a heightened risk for sharing competitively sensitive information.

Dos and Don'ts for Sharing Information	
Do seek the prior approval of your line manager before becoming a member of any trade association.	Do not remain silent. If conversation turns to dangerous territory, and a competitor or third party tries to share competitively sensitive information with you, do NOT say nothing , object, have your objection recorded in the minutes (if the meeting is minuted) and if discussions continue, leave the meeting and have your exit recorded.
Do ask for an agenda prior to attending any trade association meeting or industry event	Do not share competitively sensitive information
Do tell a member of the SLT if a competitor approaches you with a proposal to collaborate (or partner) in relation to a given job or customer. It may well be legitimate to do this, but will require careful structuring.	Do not assume that others will be as compliant, just because it was shared with you does not mean it is not problematic. Think carefully about the information that suppliers and customers (or others with whom you engage in the market) may provide to you about competitors. Is this information confidential or commercially sensitive? If so, treat it as such and do not divulge it to others.
Do ask to be placed on different teams/tables from competitors	Do not approach a supplier, technical advisor or customer to discuss or complain about the pricing practices of a competitor (for example quotes given to a competitor for the same job but where a competitor appears to have been given a more favourable price). If the supplier approaches your competitor and influences the prices that the competitor charges that could be deemed to be a price fixing arrangement between you and your competitor.

Quick Compliance: Key Dos and Don'ts for New Employees

Compliance Checklist

DO act independently in the market deciding unilaterally the price at which you quote customers, surveyors or third parties, and reject any attempt by a competitor to influence your pricing decisions.	DON'T agree with competitors the price at which you will quote or bid for work (Bid Rigging)
DO decide unilaterally , and in compliance with our practice the prices and terms at which you submit tender responses for work.	DON'T agree with competitors to share or divide markets , e.g. by allocating certain territories, customers / customer groups or products to each of you ("market or customer sharing").
DO decide unilaterally which customers / customer groups and which markets you will serve, including which tenders you will bid for .	DON'T share information with competitors concerning the price you will bid or have bid for a tender.
DO decide unilaterally on any important price and non-price terms offered to customers or suppliers, including subcontractors .	DON'T share information with competitors regarding the prices you have agreed with suppliers or subcontractors , including labour costs.
DO only participate in trade associations and industry events where appropriate safeguards are in place to prevent the exchange of competitively sensitive information.	DON'T exchange any sensitive information with competitors , e.g. regarding prices or intended increases, rebates/discounts or changes to these, terms of payment, turnover, costs (including prospective/estimated costs), marketing or other strategies.
DO exercise caution whenever you are in contact with a competitor, even on an informal or purely social level , and report any competitor contact which has caused you concern to a company director.	DON'T meet with competitors to coordinate strategies vis-à-vis your customers; and do not participate in benchmarking surveys without first having consulted your line manager, or where the survey requires you to disclose information that can be traced back to your company and reveals your company's competitive strategies, including price.
DO speak to your line manager as soon as any potential competition law concerns arise.	DON'T remain at a meeting , formal or informal, or in a group chat, or continue a discussion where your competitors engage in improper discussion on competitively sensitive matters, even if you do not actively participate in the discussion . Merely being present at an inappropriate discussion can be enough for the competition authorities to infer that you are party to an anti-competitive agreement.
DO discuss proposed agreements with competitors with your line leader before negotiations start, so they can identify any potential issues.	DON'T ask technical advisors or surveyors to share your pricing strategy with other contractors.
DO be mindful of how your communications may be misinterpreted – be clear in concise with what you say to competitors .	DON'T offer or accept cover prices from other contractors , or indicate names of "friendly" contractors to clients, manufacturers, or customers.

DAWN RAID'S ROLE BY ROLE GUIDANCE

Dawn Raids

What is a dawn raid?

A dawn raid is an unannounced investigation carried out by a regulatory authority at a company's premises or, in some cases, at an individual's home. The purpose is to gather evidence of a suspected breach of competition law—most often in electronic form, though hard copy documents may also be seized. Dawn raids typically last four to five business days, during which investigators remain on site for the duration and may ask to conduct interviews with employees of the company involved.

Who can carry out dawn raids?

In the UK, the **Competition and Markets Authority (CMA)** is the principal authority empowered to enforce competition law. However, several sector-specific regulators also hold concurrent powers within their respective industries, including: **Ofgem** (gas and electricity); **Ofcom** (communications); **Ofwat** (water); **Payment Systems Regulator (PSR)**; **Financial Conduct Authority (FCA)**; and **Civil Aviation Authority (CAA)**.

Powers of the investigators

The scope of investigators' powers depends on the type of raid and the legal authority under which it is conducted. Broadly, competition authorities may:

- Require the production of, examine, copy, and seize both electronic and hard copy documents relevant to the investigation.
- Ask questions and request explanations relating to documents.
- Take steps to prevent interference with evidence—for example, sealing rooms or filing cabinets, blocking email accounts, or suspending routine document destruction.
- Enter and search employees' private residences if they are suspected of involvement in anti-competitive behaviour, and seize personal devices and documents for offsite examination.

It is a criminal offence for a company or an individual to fail to produce or explain documents when requested, or to:

- Obstruct investigators in the course of their investigation.
- Destroy, falsify, or conceal documents.
- Provide false or misleading information.

The CMA exercises wide discretion. Obstruction can result in standalone fines (including fines of up to **1%** of a company's global turnover), increased penalties in the main case, and even personal liability for staff and directors. The safest approach is full cooperation during a dawn raid, with legal counsel present to safeguard the company's rights.

Dawn Raid Guidance

The following role specific guidance will ensure that the company's rights are protected at each stage of a dawn raid, minimising the risk to both individual employees and the company itself.

Reception/Office Coordination Staff

Dawn Raid Guidance

As reception/office co-ordination staff, you are likely to be the first point of contact when investigators arrive at the company's premises. It is essential that you set a tone of willingness to help and cooperate with the investigation.

Because dawn raids are unannounced, investigators will not have an appointment. Your role is to remain calm, cooperate fully, and follow the instructions below. Failure to cooperate can expose the company to significant penalties, including fines of up to 1% of global turnover. Please follow the steps below in order to ensure that you cooperate with the investigators and minimise the risk to both yourself and the company:

Greet the Investigators & Check their documentation
• Welcome the Investigators politely and sign them in as you would with any other visitor, but do not record the purpose of the visit • Request their identity cards and authorisation documents and take two copies of each. • Record the investigators' names, the authority they represent, the time of arrival, and any individuals they have asked to see. • Politely ask whether investigations are also taking place at other company sites. • Request the Lead Investigator's mobile telephone number. • Escort the investigators away from reception promptly. Place them in an empty meeting room until senior management arrives. Offer refreshments if appropriate. • Ask the investigators to wait for the senior management team before beginning their investigation. They will usually agree unless it is a criminal investigation or there is a risk of evidence being destroyed. If they insist on starting immediately, do not obstruct them.
Contact Management
• Contact Gary Slawson or another member of the senior management team and: ○ Ask them to come to meet the investigators as soon as possible. ○ Inform them of the key details i.e. time at which the investigators arrived, which authority they are from, how many there are and whether they have asked to see any specific individuals in the company. ○ Send them a copy of the authorisation documents. ○ Provide them with the Lead Investigator's mobile phone number.
Book Meeting Rooms
• Book out the meeting room for the entire week (ideally this rooms should not contain or provide access to the company's IT systems). • You have authority to cancel any other meetings to make space.
Confidentiality
• You should not discuss the investigation with anyone inside or outside the company, other than your management and the Knights Dawn Raid Response Team, unless you have been authorised to do so.

Never speculate or provide information beyond confirming that the management team is on its way.
Remember: your role is to facilitate access, not to answer questions about the investigation.

Management Dawn Raid Guidance

Once notified of the investigators' arrival by reception, Gary Slawson must take control immediately and assemble the internal senior management team. This is to ensure that the company cooperates fully with the investigators (avoiding any allegation of obstruction) and that the investigators act strictly within the scope of their powers as set out in the authorisation documents.

Your first step is to **contact Knights Dawn Raid Response Team (Knights)** to inform them of the dawn raid and request their attendance on site as soon as possible. This initial call should be brief as you should attend the investigators in reception as soon as possible. Notify Knights of the raid, request an estimated time of arrival and confirm you will call Knights back shortly with further details.

Charlie Markillie Partner Competition and Consumer M: 07729 094810 T: 0113 288 2734 E: charlie.markillie@knightsplc.com	Daniel Mackelden Partner Commercial M: 07776 300914 T: 01273 036343 E: daniel.mackelden@knightsplc.com
Ellen Huison Associate Competition and Consumer M: 07842 025505 T: 0113 297 8948 E: ellen.huison@knightsplc.com	Sommer Kelly Solicitor Corporate M: 07856 932407 T: 0113 288 2746 E: sommer.kelly@knightsplc.com

After making this call, you should go straight to reception to meet the investigators in person. Do not delay this step and please follow this guidance:

Contact IT - Alert the outsourced IT provider immediately and ask them to clear their diary for the rest of the week. - Ask the outsourced IT provider to come to your office as soon as possible to accompany you when meeting the investigators. - Request that they bring copies of the company's IT hierarchy to provide to the investigators. - Instruct them to halt any routine data management processes that could result in information being deleted or overwritten.
Attend to the Investigators - Go to meet the investigators without delay. - Ideally, take at least two members of the management team with you, as well as the outsourced provider (if available) to help coordinate. - Assure the investigators that the company intends to cooperate fully with the investigation. - Provide them with copies of the company sitemap, organisational chart, and IT infrastructure diagram. Ask if they require any further information at this stage. - If you have not already received it, request the Lead Investigator's mobile number. - Move the investigators to the meeting room (if not already there). Assure the investigators that this has been booked for them all week

Check the documentation • Verify that the authorisation includes the correct company name, address, and location of investigation, and that it is still valid. • Confirm that all investigators present are named in the authorisation and each has valid ID. • Check the type of authorisation document, as this determines the powers available. • Review the scope of the investigation: subject matter (e.g. products), geographic scope, and time period of the alleged infringement. • Check the type of infringement alleged; i.e. Chapter I Competition Act 1998 (anti-competitive agreements) or Chapter II Competition Act 1998 (abuse of dominance) • Establish whether it is a civil or criminal investigation. If in doubt, ask the investigators directly. • Sign the minute of notification. This only acknowledges receipt of the documents—it is not an admission of liability. If you identify errors, raise them and note that you will discuss with Knights.
Ask the investigators to wait for Knights' arrival • Request that the investigators wait for Knights and advise them of the expected arrival time. The CMA will usually wait 30–60 minutes, unless it is a criminal investigation or they fear evidence destruction. • If they agree to wait, they may impose interim conditions (e.g. sealing offices, halting data destruction, blocking email access). Agree to reasonable requests and ask the outsourced IT support to help action these. • Arrange for Knights to speak directly with the Lead Investigator by phone.
Contact Knights Dawn Raid Response Team • Provide Knights with a copy of the authorisation document (if not already done). • Share details of the raid: type of investigation, scope, authority involved, and number of investigators on site. • Confirm whether the investigators have agreed to wait for Knights' arrival. • Provide Knights with the Lead Investigator's contact details and ask them to make contact immediately.
Assemble and Brief Shadowers • While Knights will bring their own team, prepare an internal shadowing team as well. • You should brief the shadowers on the scope of the investigation, their role and their need to co-operator with the investigator • Provide each shadower with a copy of the authorisation.
Contact any Named or Key Employees • Identify the whereabouts of any individuals named by the CMA. If they are working remotely, ask them to attend the office immediately. • Identify other key employees relevant to the scope of the investigation and ensure they are on site.
Contact Staff • Confirm with the investigators that you may notify staff about the occurrence of the dawn raid. They may wish to review or approve the communication first. • Once approved, email all staff on site to inform them that CMA investigators are present and may wish to enter their offices. Instruct staff that they must comply fully and must not obstruct the investigators in any way. • Remind staff that the investigation is highly confidential and must not be discussed outside the company.

Outsourced IT Support Dawn Raid Guidance

The focus of a dawn raid has shifted decisively from filing cabinets to servers, laptops, and mobile devices. This means that a company's IT function plays a vital role in modern investigations. How quickly and accurately IT specialists can act in response to the investigators' requests will often determine whether the business is seen as cooperative and compliant, or at risk of obstruction.

Once notified of a raid by the Inspire management team or Knights, you must be ready to mobilise immediately. Investigators will often bring their own forensic experts and software tools, and they will expect rapid access to systems, data repositories, and user accounts. This makes the IT team's role critical: ensuring that investigators can carry out their work within the scope of their powers, while at the same time safeguarding the company's rights and protecting sensitive information.

Because electronic searches are time-sensitive and data-intensive, cooperation and precision are essential. Any misstep — whether accidental deletion, delay, or over-disclosure — can expose the company to significant penalties, including fines of up to 1% of global turnover and daily penalties of up to 5%. The guidance that follows is designed to help IT professionals understand their responsibilities, work seamlessly with the management team, and protect both the company and themselves during the high-pressure environment of a dawn raid.

Knights will support you with any questions you might have in respect of the investigation, the details are above.

Set up a team

- Form a team to assist and take required actions as directed by the response team leader.
- Brief all members of that Team that the company must not interfere with any steps that have been agreed with the investigators, such as blocking email accounts, suspending document deletion etc (see below).
- Assign yourself as the IT liaison to the Lead Investigator, responsible for dealing with IT and helping with facilitating access to electronic data.
- If possible, and you have the resource, assign two other members of the team, who are not assigned to shadow an investigator, to dealing with strategic requests and more difficult requests from the investigators.
- Clear your diary for the rest of the week.

Meet the investigators

Provide a thorough explanation of the IT data collection architecture to investigators, if requested. This might involve the following:

- explaining the structure of the company's IT system, how to access individual accounts from a central source and any constraints on downloading data from a central source including email systems, information stored with cloud providers, and information stored on mobile devices.
- which devices and applications are used (which may include personal devices used by staff).
- how and where the company's data is stored and how it can be accessed.
- Where requested, the IT team should (following approval from the management team) assist with: halting any routine data management processes that could result in information being deleted or overwritten.
- securing any backups.

- temporarily shutting down servers and email. This may require liaison with any external data centres which provide servers / server support.
- suspending access to certain individual or team accounts.

Set up your base

- Arrange a space that can be used as the IT operations space, from which support can be coordinated. Ideally, this space should be near to the room where the investigators are located to facilitate communication and speed of response.

Assist the investigators with appropriate access, searching, preparation of copies etc:

- Provide administrator level access to the Company's IT systems (like servers, desktops, laptops, tablets and mobile devices) and storage media (like external hard drives, backup tapes, cloud storage services)
- Assist with the collection of devices (both company and personal devices) and access to data stored offsite.
- Providing access passwords when requested.
- Enabling the investigators to operate any equipment on the premises for the purposes of searching and reviewing the company's electronic data.
- Managing the collation and production of electronic records (and retaining copies of such records to enable the response team to review following the dawn raid).
- Facilitating making forensic copies of data collected by the investigators and retain copies for the response team.

Preparing and Maintaining Records

- You should assign one member of the IT team to assist with maintaining a record of the IT requests made by the investigators. This should include when the request was made, what was requested, the deadline for complying, when the request was fulfilled and confirmation from the investigators that the step has been completed.
- You should immediately inform the management team or Knights if you are aware that the company may not be able to comply with a request within the stated deadline.

Deletion of data

- At the conclusion of the investigation, the CMA will provide the company with a forensic copy of any data that it intends to take away for review. You should confirm with the investigators how company data held on their equipment will be deleted and be satisfied that the process ensures complete and permanent removal.
- You should oversee the deletion process and request that the investigators sign a declaration confirming that any hard drives have been properly wiped.
- Make sure that all devices, hard drives or other items supplied to the CMA are returned. Where the investigators have used company-owned equipment during their search and review, this does not need to be wiped.

Shadowers Dawn Raid Guidance

“**Shadowers**” are a key part of a company’s defence of a dawn raid. Whilst it is vital that the company complies with the investigation and that no-one obstructs the investigators, each investigator should be accompanied by a shadower at all times to ensure that they do not seek to review documents which are outside the scope of the investigation (either due to subject matter or scope) or which may be covered by Legal Privilege.

You will be briefed by the management team or Knights on the scope of the authority of the investigators involved in the investigation. However, you should ensure that you have reviewed the investigators’ warrant and understand the business areas involved, the time frame covered and what and where the investigators can search.

As stated above, it is crucial that you do not take any steps that could be seen as obstructing the investigation. Companies which obstruct an investigation can face fines of up to 1% of global turnover and/or daily penalties of up to 5% of daily global turnover. As such, you should not seek to interfere or obstruct the investigation in any way and should not engage in unnecessary conversation with the investigators unless specifically asked to do.

Following the below guidance will ensure that you protect the interests of the company during the investigation and also avoid any allegations of obstruction against yourself or the company.

General Responsibilities
<u>Know the scope of the investigation</u> as set out in the investigation decision/warrant. Always accompany and watch the investigator. <u>Record in writing</u> all the investigators’ investigation activities. <u>Keep checking</u> whether the investigators’ activities are covered by the warrant; <u>if the investigator seeks to look at documents outside of scope, object and liaise with Knights</u> <u>Be polite, but firm</u> and tactful in the situation. Each Shadower should <u>follow their allocated investigator</u> and should not allow them to wander off alone.
Carry with you:
Mobile phone. Mobile number of management team/ Knights contact. This leaflet. Copy of search warrant/decision.
Providing guidance to employees being searched
investigators <u>must be granted access</u> to offices and computers. Employee being searched may leave the office during the search (no obligation to be present). At the investigators’ request, <u>employee must hand over cabinet keys / passwords / documents</u>, provided such request is within the scope of the investigation (e.g. in terms of relevant period). Employees should not give answers concerning the subject matter or sign documents <u>without prior legal advice (see below)</u>. Try to <u>reduce talks</u> between employees and investigators <u>to a necessary minimum</u>; permissible questions may concern group structure, whose desk is in which room, employee functions, location of documents etc. Documents or computer files must not be removed, manipulated or destroyed.
Responsibilities during document searches
<u>Record in writing</u> as comprehensively as possible all the investigators’ activities, in particular: Who is being searched? What is the investigator looking for? What documents shall be copied? Any peculiarities?

Keep checking whether documents reviewed are covered by the scope of the investigation (e.g. alleged offence, time period, geographical area, companies concerned); if necessary, object and contact the Head of Legal.

Make copies (if possible two) of all the documents seized.

Legal Privilege: Claim legal privilege for documents produced by / for a lawyer or for communication with a lawyer (such documents must not be reviewed / seized by the investigators); legal rules on privilege vary, depending on jurisdiction / type of dawn raid; liaise with Knights if investigators disagree.

Responsibilities during E-searches (PCs, notebooks, servers)

- **Record E-search as comprehensively as possible** (“looking over the shoulder”): Whose and which data / accounts are being downloaded / searched / printed? Which search terms are used? investigators are not required to reveal a list of search terms but may not conceal search terms appearing on screen.
- **Carefully watch** the review of any electronic data, including where this is done on the investigators’ own IT equipment.
- Keep checking whether search terms, selected files and data are **covered by the scope of the investigation**; if necessary, object and contact the Knights.
- Inform Knights if investigators want to **access external servers or copy unsearched data** records to storage devices (e.g. USB stick / hard drive) and take it along.
- **Legal Privilege:** Object if the investigators seek to review documents/emails which contain legal advice.

Questioning of Employees

- investigators may ask questions relating to the **location of documents or factual questions** to help them understand the document on its face.
- If the investigators want to ask questions relating to the subject matter only of the investigation, politely ask that they wait until External Legal are present.
- Keep detailed documentation of the interview including questions asked and answers given.

Searched employees Dawn Raid Guidance

If investigators of an authority (e.g. the CMA) search your office / computer in connection with an investigation in connection with a suspected breach of Competition Law (“**dawn raid**”), **please keep calm, be friendly, do not obstruct the investigation, do not provide informal guidance / information**, and observe the following instructions:

- **Unaccompanied investigators**: If the investigators are not accompanied by a member of Knights specifically trained for on-site investigations (so-called “**shadowers**”), please contact the management team immediately and explain to the investigators that your call is purely intended to inform the responsible contact. Explain to the investigators that you wish to have a shadower present during the search of your office and / or computer. Should the investigators ignore your request, **DO NOT** put up any resistance but ask them to document your request.
- **DO NOT destroy, manipulate, or hide documents or files**: Such actions may be treated as obstruction, a criminal offence, punishable by fines and personal sanctions. You should also avoid any behaviour that could be misinterpreted (e.g. routine shredding).
- **Follow the instructions of the shadower**: The Shadower's role is to follow the investigators and make sure they do not exceed their powers. There is no obligation for you to be present during the search, however the Shadower will decide whether you should be present.
- **Information on where to find documents or on passwords to be provided only after consultation with the shadower**: The investigators are authorised to request access to documents and files which are relevant to their searches. Where possible you should **first consult with the Shadower** before you provide information to the investigators on the storage location of documents and before you disclose your electronic access data such as passwords.
- **Only answer questions following consultation with the Shadower**: If questions move away from factual explanations of a document and instead go towards the subject matter of the investigation you should ask the investigators to wait until Knights are present.
- **DO NOT sign anything** unless discussed with the Shadower.
- **DO NOT inform competitors / other companies** about the ongoing investigation at your site.
- **DO NOT interfere with or obstruct** the investigation in any way.
- **DO NOT prevent the investigators from accessing relevant documents, computers, mobile or electronic devices or property.**
- **DO NOT engage in unnecessary conversation** unless specifically asked to do so with the investigators.

Domestic Premises Dawn Raid Guidance

In certain circumstances, CMA investigators may also have the power to enter and undertake an investigation of an individual's domestic premises (potentially including vehicles), provided they have obtained a valid warrant. Where a warrant is obtained for these purposes, the CMA has broader powers of investigation, allowing them to force entry into your premises and actively search for relevant documents, as opposed to requiring their production. Therefore, it is important that you act fast to control the situation but do not overstep the mark by interfering with the CMA's investigation in any way.

Although it can be extremely unsettling to see investigators arrive at your home to carry out a dawn raid, it is important that you remain calm and co-operative and follow the steps outlined below. Failure to cooperate with the investigative measures will not only expose the company to the potential of significant penalties but it may also result in serious criminal penalties for you as an individual, including fines and imprisonment. Please ensure that you follow the below guidance in the event that the CMA arrive at your home to conduct an investigation:

Check the warrant

- Ask the investigators to provide you with the warrant obtained for the search and take a photo of the warrant (to send to the management team) – investigators are not entitled to enter and search domestic premises without a valid warrant.
- Check that the warrant:
 - relates to the premises the investigators are seeking to enter and search;
 - identifies all of the attending investigators as being authorised to investigate; and
 - lists the scope of the investigation (confirm this with the investigators as well)

Take a photo of the paperwork if the investigators do not have a photocopy.

As the Lead investigators for their name and mobile phone number.

If the warrant appears to be invalid then contact the management team/Knights immediately.

Contact the Management Team for assistance

- Call the management team to inform them that the CMA is at your home and confirm to them:
 - how many investigators are present; and
 - the scope of the investigation (by sending them a photo of the warrant or reading it to them).

Provide them with the name and phone number for the Lead investigators.

Ask the management team to contact Knights Dawn Raid Response Team immediately.

If the management team is not available, then call Knights external legal counsel directly.

Check identification

- Ask each CMA investigator to provide you with their full name and their identification.
- Take a photo or copy of each ID document.
- Check that the details on the warrant correspond with the ID documents of the attending investigators.

Request that the CMA investigators wait for Knights external legal counsel to arrive

- Tell the investigators how long you expect it will take for legal support to arrive and ask the investigators if they would be willing to wait for them to arrive before they commence the investigation.

- They will generally wait a reasonable time (typically 30-60 minutes), unless it is a criminal investigation.
- If they do not, ask them if they will speak with external legal counsel themselves to confirm the focus of their search.
- Do not prevent the investigators from commencing their search if they do not agree to wait for external legal counsel or are unwilling to speak to them

Keep a full record of events during the search

- Ensure that you maintain a full record of events during the investigation including:
 - the documents (both electronic and paper) reviewed by the investigators;
 - IT equipment accessed and searched (both business and personal devices)
 - any particular areas they seem interested in;
 - any points of dispute.
- If they attempt to ask you any questions you should ask the investigators to allow you to respond to these once support has arrived.
- If you are unsure whether or not to comply with any requests from an investigator, check first with Knights.

Things to avoid if CMA investigators arrive at your home:

Don't try to prevent the investigators from entering if they have a valid warrant.

Don't destroy, delete, falsify, or conceal any documents (including any electronic records in any format e.g. text messages, emails and voice messages).

Don't inform anyone outside of your company or Knights about the investigation

Don't allow the investigators to wander off unaccompanied in your premises.

Don't allow the investigators to review documents which are legally privileged or outside the scope of the investigation.

Don't enter into any unnecessary conversations with the investigators apart from what is contained within the guidance above.

Knights Dawn Raid Response Team: Contacts

Charlie Markillie Partner Competition and Consumer M: 07729 094810 T: 0113 288 2734 E: charlie.markillie@knightsplc.com	Daniel Mackelden Partner Commercial M: 07776 300914 T: 01273 036343 E: daniel.mackelden@knightsplc.com
Ellen Huison Associate Competition and Consumer M: 07842 025505 T: 0113 297 8948 E: ellen.huison@knightsplc.com	Sommer Kelly Solicitor Corporate M: 07856 932407 T: 0113 288 2746 E: sommer.kelly@knightsplc.com