Confidential Information and Trade Secrets – What are they and how can they be protected?

Confidential information and trade secrets can be integral to the success of businesses in all industries as they bid to outperform their competitors. As such it can be vital for businesses to understand the law as it applies to confidential information and trade secrets, and to take adequate steps to ensure that they are properly protected. This article summarises the circumstances that give rise to the existence of confidential information and trade secrets, and gives examples of some practical steps that can be taken to ensure their protection.

Confidential Information

The law as it relates to confidential information is built upon the equitable principle that a person who has received information in confidence cannot take unfair advantage of it, and must not use it to the detriment of the person who provided the information, without their consent. Confidential information can in theory be protected indefinitely, so long as it retains its confidential nature.

In the UK there is a three-stage test to determine whether information can be categorised as confidential[1]:

1. The information must have the necessary ‘quality of confidence’

   This requirement excludes information that is already in the public domain or that can be readily deduced from pieces of information that are publicly known. On the other hand, applying skill and ingenuity to the way in which public domain materials are put together can create something (such as a customer database or a new formula or recipe) that does deserve protection as confidential information.

2. The information must be imparted in circumstances importing an obligation of confidence

   A recipient of confidential information should know, or should realise from the circumstances, that the information provided to them is confidential, and that they are required to keep it secret. Confidentiality agreements or non-disclosure agreements (“NDAs”) can be entered into in order to explicitly state that imparted information is to be treated as confidential. In the absence of an NDA, an implied duty to maintain confidentiality can arise, either because in the circumstances of the disclosure the reasonable person would have realised that the information was confidential, or because of the special relationship between the parties, for example that between an employer and an employee who routinely deals with confidential information in the course of their job.
3. **There must be unauthorised use or disclosure of the information that is detrimental to the owner of the information**

The confidential information must be used or disclosed (either threatened or actually) in an unauthorised manner and thereby cause harm to the owner, for example by eradicating a commercial advantage. This can include circumstances in which information was disclosed for one purpose but is used by the recipient for another.

Many different types of information can be confidential provided that they meet the three-stage test above. Examples include:

- product formulae and recipes;
- operating procedures, policies and practices;
- secure codes and algorithms;
- research and development projects;
- financial information and business plans;
- customer and supplier information;
- employee information including salaries; and
- some or all terms of commercial agreements and settlement agreements.

In some cases, the existence of the item (such as a research project or settlement agreement) can be confidential as well as the details.

**Trade Secrets**

A trade secret is a particular type of commercially valuable confidential information that gives the owner a competitive advantage. There is considerable overlap between the common law confidential information regime discussed above, which recognises trade secrets as a subset of confidential information that would cause serious harm if improperly disclosed, and the protection afforded by the Trade Secrets (Enforcement, etc) Regulations 2018[2] ("Trade Secrets Regulations").

The Trade Secrets Regulations define trade secrets as being information which:

1. is secret (i.e. is not generally known or readily accessible to persons within the relevant circles);
2. has commercial value because it is secret; and
3. has been subject to reasonable steps to keep it secret.

While the first part of the definition is wider than that for trade secrets at common law, the third part is narrower. It also requires owners of confidential information to identify the trade secrets within it and then implement reasonable steps to protect them before they can take advantage of the Trade Secrets Regulations[3]. Those advantages primarily relate to enforcement proceedings and remedies.

**Remedies available for unlawful use of Confidential Information and Trade Secrets**

**Injunction** – Interim as well as final, post-trial injunctions can be sought to prevent confidential information (including trade secrets) from being unlawfully disclosed or used, either where this is threatened or has already
happened, as well as to enforce the destruction or delivery up of any physical embodiment of the information. Note that once disclosure or use has taken place there may be little or no value in seeking an injunction.

**Damages** - Damages can be awarded to rectify economic loss caused by the unlawful disclosure or use of confidential information. The usual measure of damages is that the defendant should fairly compensate the claimant for that loss, regardless of whether this is in the form of lost profits or licensing income etc.

**Account of profits** - As an alternative to damages, an aggrieved party can claim the profits accrued by the unauthorised party through the unlawful disclosure or use of the information.

**Compensation and publicity orders** - These additional remedies are available under the Trade Secrets Regulation. A person who innocently used another's trade secrets can apply to the court asking that, rather than be enjoined or have to destroy or deliver up goods, it pays compensation to the injured party. Following trial, a trade secret holder can request the court to order dissemination of information about the judgment at the expense of the person found to have misused its trade secrets. This can be in the form of a notice on the infringer’s website or in trade journals and can be valuable in correcting any public misperceptions about a case.

**Practical steps to protect Confidential Information and Trade Secrets**

- Contracts such as NDAs can be entered into to protect information and allow for a contractual right to an injunction and a damages claim in the event of a breach of the contract’s terms. As well as entering NDAs with third parties, it is always prudent to set out employees' and consultants' duties in relation to confidential information and trade secrets in their service contracts to make it clear what those duties are and what information is covered by them. A contractual obligation is generally easier to enforce than a claim under the common law or Trade Secrets Regulation.
- A business should have a clear and thorough confidentiality policy in place. Employees should be aware of the policy and receive training on how it is applied and how it should be complied with. By way of example, employees should be advised not to discuss company business on public transport and to take care when using laptops or mobile devices in public places. Additional measures for the protection of trade secrets should also be set out.
- A register of confidential information can be created and maintained in order to create clarity within a business as to what is deemed confidential and what warrants the higher level of protection of a trade secret.
- It is good practice to limit the disclosure of confidential information, and particularly trade secrets, to identified individuals who need to use it to carry out their roles. Security systems should also be put in place to ensure that confidential information, and again particularly trade secrets, can only be accessed by permitted recipients. Electronic security measures that can be used include firewalls, secure emails, passwords and encryption.
- There should also be an appropriate action plan in the unfortunate event that the aforementioned security systems are breached or some other circumstance results in an unauthorised disclosure.

---


[3] There has not yet been any court guidance on what constitutes “reasonable steps”. It will depend on the nature of the information, business and circumstances, though would include matters such as restricting and
monitoring access to the trade secrets, training staff and having appropriate confidentiality terms in employment, consultancy and other contracts.