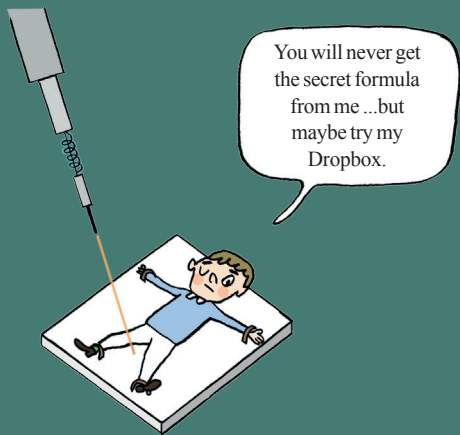


CM | MURRAY

The Little Book of
**Confidential
Information**



Welcome	4
What is Confidential Information?	6
Categories of Business Information	9
The Prudent Employer	12
The Prudent Employee	18
Dealing with Breaches of Confidentiality	19
Take Advice from Us	26
About the Team	28

Welcome

We thought it would be helpful to create a Little Book which focuses on the issues, risks and practical handling for businesses and senior employees relating to the misuse of confidential information.

If you are facing an issue relating to misuse of confidential information, it is very important you take specialist advice early – please do contact us and we will be very pleased to discuss how we can help you.

Very best wishes

The Team at CM Murray LLP

info@cm-murray.com | +44 (0)207 933 9133

This booklet is only a brief overview of relevant English employment law and is for general purposes only. Specific legal advice should be taken on particular circumstances. Please do contact us and we would be pleased to help you. Information correct as of May 2018.

Encryption Man
will safeguard
your confidential
information.



Not if I, Captain
Blabbermouth,
strike first!



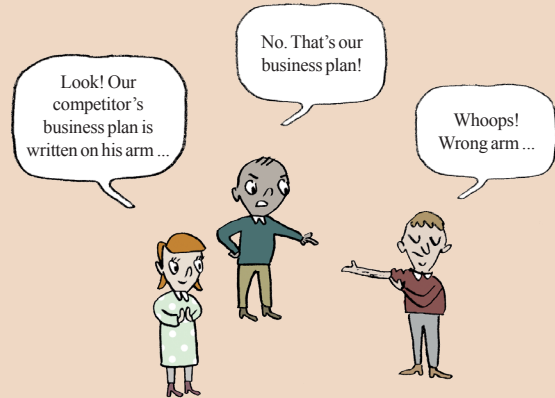
What is Confidential Information?

All businesses have confidential information of one type or another. Typical examples include:

- Secret recipes, designs, processes or formulae
- Lists of customers, suppliers and other contacts
- Pricing and other financial information
- Business strategy and plans

Because employees need to access and use the information for the benefit of the business, there is a risk it will be misused for the employees' own purposes, or that it will fall into a competitor's hands.

However there are steps employers can take to protect this important asset.



Categories of Business Information

There are five different categories of business information. Whether particular information can be protected, and how, depends on which category it is in. The categories are:

- **Trade secrets** – these can be protected both during and after employment. Employees have an implied obligation not to misuse or improperly disclose trade secrets at any time, so employers can protect them even without an express contractual term.

- **Other Confidential Information** – this is information which isn't a trade secret but is still sufficiently confidential to require protection.

Employees have an obligation not to misuse or improperly disclose this type of information during their employment due to the implied duty of fidelity that every employee owes, but an express contractual term is needed to protect the information once the employment has ended.

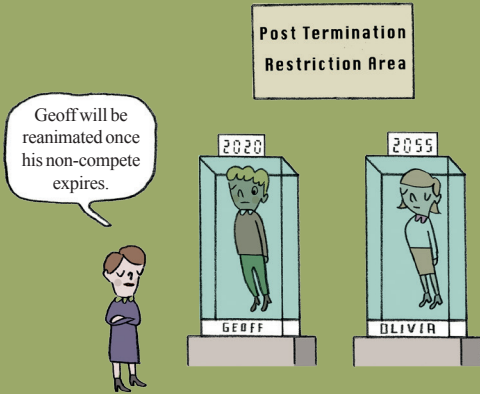
The express contractual term must be carefully drafted, otherwise it could be unenforceable.

- **Skill and knowledge** – information which amounts to the skill and knowledge of an employee belongs to the employee, and he or she is free to use it
- **Public information** – information about the employer's business which is in the public domain cannot be protected
- **Databases** – these have special protection under legislation. Although the definition of a “database” is complicated, an electronic, systematic record maintained by an employer (e.g. a CRM database) is likely to be covered. Unauthorised extraction or reuse of the information in a database could lead to an award of penal damages

The Prudent Employer

Here are some things employers can do to safeguard their confidential information, and increase the chances of the information being protected by the Courts if legal proceedings become necessary:

- Include **express confidentiality obligations** in employees' contracts, to apply both during and after the end of the employment
- **Define** the types of information which are protected as **precisely** as possible, and with sufficient scope to cover all that needs to be protected



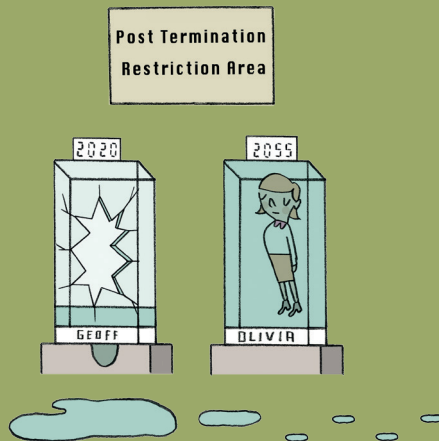
- **Restrict access** to particular confidential information to those employees who actually need it in performing their job
- **Mark sensitive documents**, emails etc. “confidential”
- Use **password protection** on confidential electronic documents, and keep hard copies in a locked drawer or cabinet
- **Restrict the taking** of documents out of the workplace without authorisation
- **Adopt policies** which prohibit the sending of business information to personal email accounts, and the use of USB sticks or other storage devices in the workplace

- **Monitor IT systems** for excessive downloads of information and other unusual activity

Agreeing some further **post-termination restrictions** with particular employees could also help protect the business's confidential information. These could include restrictions against:

- Working for competitors
- Soliciting and dealing with certain clients

for a limited and reasonable period after the employment has ended. Such restrictions will need to be drafted carefully, otherwise they could be unenforceable.



Eye of Newt,
Toe of Frog
and ... ?



Sorry,
I'm subject
to a Witch's
Covenant.



The Prudent Employee

Employees must resist any urge to use their employers' confidential information for their own purposes or to pass it on to their next employer.

The chances of being caught are high, especially where there is some electronic trace of the employee's activities, and the potential consequences of any legal action could be very damaging.

Dealing with Breaches of Confidentiality

Employers who suspect an employee has breached, or is preparing to breach, their obligations of confidentiality should take legal advice as soon as possible. If an employer bides its time, this could restrict its options.

An **employee** who is accused of breaching confidentiality should also seek legal advice quickly, as the employer might begin legal proceedings if the matter isn't taken seriously or the employee reacts in the wrong way.



If the employee has committed a breach, he or she must **preserve any evidence** of the breach, and must not try to cover it up (e.g. by deleting incriminating emails or destroying documents). Deletion is generally pointless anyway and often makes things worse, because it is very hard to delete emails and documents so well that they cannot later be recovered by computer experts.

The **accused employee** might be asked to:

- Give **written undertakings** to comply with their confidentiality obligations.
- Give a **full account** of what information they have taken and what they have done with it, possibly in a sworn statement or affidavit.

- **Deliver up** the information taken
- Allow the **forensic examination** of any personal IT equipment, storage media or email account on which the confidential information has been held

If the employee ignores the request or is evasive, or if there is another pressing need, the employer could seek an **injunction** from the Court.

This could require the employee to take particular steps or refrain from certain action, and any breach of the Court's order could result in the employee being **fin**ed or **sent to prison** for contempt of court.

The employer might also pursue a claim for **damages** for any losses it has suffered, or for an **account of profits** if the employee has benefited from misusing the confidential information.



Where the employee has misused confidential information to gain an advantage or head start in another business, the Court could grant a **springboard injunction** to prohibit the employee from being involved in that new business for a period of time, to remove or limit this advantage.

If the **employee's new employer** is alleged to have induced or encouraged the employee's breach of confidentiality, it might also be brought into the proceedings.

Take Advice from Us

Whether you're an **employer** looking to safeguard your confidential information, or a senior **employee** who needs to understand your obligations, don't leave it too late to get the right advice. **Contact us** without delay and we'll be ready to help.

About the Team



Clare Murray
Managing Partner
clare.murray@cm-murray.com
+44 (0) 207 933 9134



Sarah Chilton
Partner
sarah.chilton@cm-murray.com
+44 (0) 207 933 9125



Anna Birtwistle
Partner
anna.birtwistle@cm-murray.com
+44 (0) 207 933 9121



Esther Martin
Partner
esther.martin@cm-murray.com
+44 (0) 207 933 9120



David Fisher
Partner
david.fisher@cm-murray.com
+ 44 (0) 207 933 9122



Samantha Mangwana
Partner
samantha.mangwana@cm-murray.com
+ 44 (0) 207 933 9139



Beth Hale
Technical Director
beth.hale@cm-murray.com
+44 (0) 207 933 9131



Nick Hawkins
Associate
nick.hawkins@cm-murray.com
+44 (0) 207 933 9122



Wonu Sanda
Associate
wonu.sanda@cm-murray.com
+44 (0) 207 933 9124



Zeinab Harb
Trainee Solicitor
zeinab.harb@cm-murray.com
+44 (0) 207 933 9126



Naomi Latham
Paralegal
naomi.latham@cm-murray.com
+ 44 (0) 207 933 9137

CM Murray LLP is a specialist UK
Employment & Partnership law firm.

Chambers and Partners:

Ranked Band 1 for Employment: Senior Executives
& Corporate & Commercial: Partnership

“This ‘hugely innovative’ employment and partnership boutique has recognised strengths in advising clients on City team moves, high-value discrimination claims and senior executive exits. It has a notable presence in the financial and broadcasting sectors.

The team frequently handles cross-border matters for both individuals and corporates.”

Legal 500:

Ranked Tier 1 for Employment: Senior Executives
& Corporate & Commercial: Partnership

“The firm specialises in acting for firms and individuals in distress situations, where there are serious threats to reputation and where there are multiple jurisdictions involved.”

CM Murray LLP

First Floor, 36–38 Cornhill, London, UK EC3V 3NG

www.cm-murray.com

T: +44 (0) 207 933 9133

Out of hours: +44 (0) 7957 383079

Twitter: @CMMurrayLLP

Illustrations by David Orme dorme@hotmail.co.uk

Design by toucari.live