

Bird & Bird

Trade Secrets Top Tips

Protect your trade secrets and other IP in a global workplace throughout the employment lifecycle



At the start of and during employment



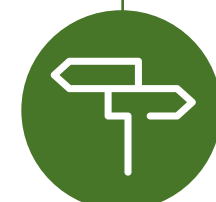
Clear policies and contractual terms

- Check template employment contracts, employee handbooks and company policies:
 - contain **clear wording** to protect your confidential information, trade secrets, and other IP;
 - are kept **up to date** with changes in the law in all countries where your business operates; and
 - reflect the global workplace of remote and hybrid work.
- **Review** whether separate NDAs need to be signed by any employees working in senior or sensitive roles or handling highly confidential information.
- Ensure any post-termination restrictions (eg non-compete, non-solicitation) in the employment contract are **tailored, well-targeted and properly informed** by the actual needs of the business and the specific role of an employee.



Identify and audit valuable trade secrets and other IP

- Conduct a **regular audit** of your confidential information, trade secrets and other IP and identify:
 - what are your confidential materials and trade secrets?
 - where are they held?
 - who has access to them?
 - what IP does the business actually own and use?



Labelling

- Clearly **label** such information with confidentiality warnings and/or with copyright notices and make it clear that they are not for external disclosure.
- **Record** who has control and access to this information and who owns/develops IP within the business – records of drafts and historic documents can be useful to demonstrate ownership of IP.



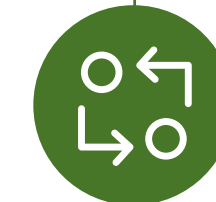
Restrict access

- Use physical or digital restrictions, sign off requirements and download limitations to **restrict access** to trade secrets and other IP.
- Consider **limiting access** to a “need to know” basis.



Educate employees

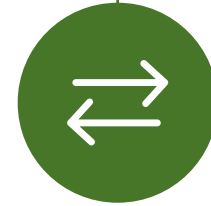
- Deliver regular (eg annual) IT/compliance and/or trade secrets awareness training to **educate and remind** employees about:
 - the importance of protecting trade secrets and other IP, and how their actions might impact that protection;
 - data security and the difference between personal and corporate devices; and
 - their contractual obligations to protect confidential information and other IP.



Develop a strategy

- Establish a clear **business disaster response plan and strategy** to act quickly if information is taken.
- Consider **monitoring** employees’ IT use to help identify potential breaches or issues quickly (eg large volumes of printing, big downloads or many emails to personal accounts).

At the end of employment



Implement offboarding procedures

- Establish and **implement structured and clear offboarding procedures** for outgoing employees. This may include:
 - **written reminders** to staff about their non-disclosure obligations and contractual duties in relation to confidential information, trade secrets and other IP;
 - the **immediate return and/or deletion** of company information, property and IP, including (if required) the assignment in writing of IP;
 - **trade secrets awareness training** as part of an exit interview;
 - utilising **garden leave** to restrict employee activities during their notice period and/or **deferred compensation payments** (if relevant); and
 - where appropriate, **notifying the new employer** of the employee's contractual obligations and restrictions of the business and the specific role of an employee.



Act quickly if there is a potential threat

- Assess and minimise the impact internally (on staff) and externally (on clients, customers and suppliers);
- Reinforce existing business relationships;
- Identify, collect and secure evidence (eg computer and/or phone records) engaging specialist computer forensic experts if appropriate;
- Investigate possible employee misconduct and consider suspension and/or disciplinary action (if applicable);
- Work out what evidence there is of any wrongdoing and where it might be; and
- Assemble the appropriate team of advisors to tackle the threat.



Organise

- Organise an internal management team, involve legal and if necessary, notify insurance providers.

Bird & Bird

One firm. Your firm.

[twobirds.com](https://www.twobirds.com)



Olivia Baxendale
Professional Support Lawyer

T +44 20 7415 6680
E olivia.baxendale@twobirds.com



Tim Spillane
Partner

T +44 20 7905 6304
E tim.spillane@twobirds.com



Kate Hurn
Senior Associate

T +44 20 3017 6918
E kate.hurn@twobirds.com



Louise Sargeant
Senior Associate

T +44 20 7905 6327
E louise.sargeant@twobirds.com

The information given in this document concerning technical legal or professional subject matter is for guidance only and does not constitute legal or professional advice. Always consult a suitably qualified lawyer on any specific legal problem or matter. Bird & Bird assumes no responsibility for such information contained in this document and disclaims all liability in respect of such information. This document is confidential. Bird & Bird is, unless otherwise stated, the copyright owner of this document and its contents. No part of this document may be published, distributed, extracted, re-utilised, or reproduced in any material form. Bird & Bird is an international legal practice comprising Bird & Bird LLP and its affiliated and associated businesses. Bird & Bird LLP is a limited liability partnership, registered in England and Wales with registered number OC340318 and is authorised and regulated by the Solicitors Regulation Authority. Its registered office and principal place of business is at 12 New Fetter Lane, London EC4A 1JP. A list of members of Bird & Bird LLP and of any non-members who are designated as partners, and of their respective professional qualifications, is open to inspection at that address.