RDS
ADVOCATES & SOLICITORS

In Business Collaboration:
AMT / ANDERSON MORI & TOMOTSUNE

Confidentiality At Work: Where Does An Employee's Knowledge End And An Employer's Secrets Begin?

18 September 2026

For more information, please contact:

Rajeswari Karupiah
rajeswari@rdslawpartners.com

Muhamad Sharulnizam
sharul@rdslawpartners.com

As employees move between companies, use personal devices and increasingly turn to generative AI, employers face growing challenges in protecting confidential information. But while businesses can protect their trade secrets and proprietary information, they cannot expect employees to leave their skills and experience behind when they resign.

The employment relationship may end, but an employee's obligations concerning confidential information do not necessarily end with it.

For employers, the challenge lies in drawing the line between information that belongs to the business and the knowledge, skills and experience that an employee is entitled to carry throughout their career.

This topic took centre stage at the recent RDS Employment Law Client Briefing 2026 during a panel discussion on confidentiality and breaches of employment agreements.

The Employee's Duty Goes Beyond The Contract

During employment, an employee's obligations are governed by both the employment contract and common law duties of good faith and fidelity.

Employers should therefore ensure that their employment agreements address confidentiality and non-disclosure, ownership of intellectual property created during employment, return and deletion of company information, conflicts of interest and, where appropriate, non-solicitation obligations.

But contractual terms are only part of the picture.

An employee remains expected to act in the employer's interests during the employment relationship and not deliberately act against the employer's business.

The more difficult question is what happens when the employee resigns. Employees are entitled to take their professional skills, knowledge and experience with them.

What they cannot necessarily take is the employer's specific confidential information.

Dr Bahari illustrated the distinction using popular culture: an employee's skill and experience are like the abilities of a professional operative - they reside in the individual. The employer's confidential dossier, however, is something different: specific information belonging to the organisation.

The same principle applies to professional expertise. An employee may leave with the ability to perform a particular task, but that does not mean they are free to take the employer's confidential customer database, pricing information, tender strategy or technical documentation.

The distinction is particularly important when employees move to competitors or establish competing businesses.

"Confidential" Does Not Automatically Mean Confidential

Employers should also avoid relying solely on labels. The classic test in Coco v A N Clark (Engineers) Ltd *[1968] FSR 415; [1969] RPC 41* asks whether:

1. the information has the necessary quality of confidence;
2. it was imparted in circumstances giving rise to an obligation of confidence; and
3. it was used in a manner causing detriment to the owner.

In practical terms, an employer should be able to demonstrate that information is genuinely confidential and has been treated as such.

A document marked "CONFIDENTIAL" but circulated freely throughout the organisation, left unsecured or effectively placed in the public domain may be difficult to protect.

Conversely, the absence of a "CONFIDENTIAL" stamp does not necessarily mean that information loses its confidential character. The nature of the information and the circumstances surrounding it remain important.

The Courts Look At The Facts

There is no single rule determining what an employee can and cannot take. The panel highlighted several cases illustrating the fact-sensitive approach adopted by the courts.

In Worldwide Rota Dies Sdn Bhd v Ronald Ong Cheow Joon [2010] 8 MLJ 297 (HC), a senior employee took the employer's client list to a new company for his own enterprise. The court found that the client list belonged to the employer.

In Dynacast (Melaka) Sdn Bhd v Vision Cast [2016] 3 MLJ 417; [2016] 6 CLJ 176 (FC), however, the court took a different view. The former employee had extensive experience in the relevant industry and the information relied upon was found to be within general knowledge. The employee was therefore able to perform the work based on his own experience rather than stolen confidential information.

In IEM SA v Flowbird Malaysia [2026] 1 MLJ 582 (CA), the court found that information including pricing, contractual conditions, budgets a d other contractual data constituted confidential information in circumstances involving a competing business.

The message for employers is clear: the question is not simply whether an employee knows something. It is what the information is, how it was obtained, whether it was confidential and how it was used.

A Breach Does Not Have To Be Malicious

Confidentiality breaches do not always arise from deliberate attempts to steal information.

An employee may inadvertently expose confidential information to third parties, particularly in an environment involving cloud systems, personal devices and remote working.

One must also pay attention to the importance of controlling not only actual disclosure but also the risk of unauthorised third-party access.

For example, an employee who places company information on an inadequately secured system may expose that information even if no outsider ultimately accesses it.

This is why employers should ensure that their internal policies address unauthorised access, storage and exposure of confidential information, rather than focusing only on deliberate disclosure.

Personal Data Adds Another Later Of Risk

A confidentiality breach and a personal-data breach are not necessarily the same thing. However, where confidential information contains personal data, an incident can create an additional set of risks for the organisation.

The distinction lies partly in who suffers the harm. A confidentiality breach may primarily affect the party to whom the confidentiality obligation is owed, while a personal-data breach can affect the individuals whose personal data has been compromised.

Businesses handling significant amounts of personal data should therefore consider data minimisation, access controls and limiting the amount of personal information employees can access or use at any particular stage of the data life cycle.

AI Is The New Confidentiality Frontier

Generative AI has created a particularly difficult problem for employers. An employee may upload a confidential document to an AI platform simply to obtain a summary, improve drafting or analyse information.

From an employer's perspective, however, once confidential information is submitted to an external AI system, control over that information may be compromised. There may also be intellectual-property concerns where AI-generated material incorporates or reproduces information belonging to another party.

Clearly, employees should not upload company confidential information into generative AI tools unless the employer has expressly authorised it and appropriate safeguards are in place.

However, employers must also consider the employment-law dimension. If there is no clear policy prohibiting such conduct, it may be more difficult to establish that an employee has breached an express or implied term of employment.

A clear AI policy should therefore address what employees can and cannot upload, which approved tools may be used, what information is prohibited and the consequences of non-compliance.

Does A Confidentiality Breach Justify Dismissal?

Not automatically.

Dismissal is the most serious disciplinary penalty and should generally be proportionate to the misconduct. The seriousness of a breach will depend on factors such as:

- the sensitivity of the information;
- the extent of disclosure;
- whether the conduct was intentional or inadvertent;
- the actual or potential consequences;
- the employee's seniority and responsibilities;
- whether the employee had received appropriate training or warnings; and
- the employee's disciplinary history.

Consistency also matters.

An employer that previously treated similar misconduct leniently may face difficulties imposing a substantially more severe penalty in a subsequent case without good reason.

The circumstances of a junior employee inadvertently posting an image of a sensitive workplace area will obviously differ from those of a senior employee deliberately taking tender documents to a competitor.

What About Customers Who Follow An Employee?

A departing salesperson cannot simply assume that all customers they dealt with during employment are theirs to take.

If the employee downloads or removes the employer's customer list or uses proprietary customer information to solicit business for a competitor, the employer may have grounds to take action.

This does not mean an employee can never continue a genuine professional relationship with a customer after leaving. The distinction is between the employee's personal professional relationship and the employer's proprietary information.

Employers can also take practical steps during a lengthy notice period. For senior employees considered a significant risk, garden leave may be appropriate, together with restrictions on system access.

At the same time, employers should consider engaging key customers directly to reassure them that the business remains capable of servicing their needs.

What Should Employers Do?

The discussion points to several practical steps:

- Review employment agreements to ensure confidentiality, IP ownership, return-of-information and post-employment obligations are appropriately drafted.
- Identify critical confidential information and determine who has access to it and how it can be removed or transferred.
- Strengthen technological controls, particularly for personal devices, cloud systems and remote access.
- Establish clear AI policies before an AI-related incident occurs.
- Train employees on confidentiality, social media, cybersecurity and AI use.
- Review exit procedures for departing employees, including access restrictions, return of devices and deletion of company information.
- Apply disciplinary measures consistently and proportionately when breaches occur.

Conclusion

Confidentiality is no longer simply a matter of keeping documents in a locked filing cabinet.

Information can leave an organisation through a personal phone, a screenshot, a social-media post, an unsecured server or an AI prompt.

Employers therefore need more than a well-drafted confidentiality clause. They need clear policies, effective technological controls, employee training and a disciplined approach to managing departures.

At the same time, employers should recognise the limits of what they can protect. An employee's professional skills, knowledge and experience are not the employer's property.

The real challenge is identifying where legitimate professional know-how ends and confidential business information begins and putting the right safeguards in place to protect that boundary.

KUALA LUMPUR
Level 16, Menara 1 Dutamas No. 1, Jalan Dutamas 1, Solaris Dutamas, 50480 Kuala Lumpur
T: +603 6209 5400
F: +603 6209 5411
enquiry@rdslawpartners.com

PENANG
Suite S-21E & F21st Floor, Menara Northam, No. 55, Jalan Sultan Ahmad Shah, 10050 Penang
T: +604 370 1122
F: +604 370 5678
generalpg@rdslawpartners.com

JOHOR BAHRU
8-35, Menara Delima Satu, Jalan Forest City 1, Pulau Satu, 81550 Gelang Patah, Johor Bahru
T: +607 585 6414
F: +607 509 7614
generaljb@rdslawpartners.com