



CM ADVOCATES LLP



NON-DISCLOSURE AGREEMENTS IN THE AGE OF REMOTE WORK

The shift to remote and hybrid working has changed how businesses access, use and share confidential information. Employees now handle client information, financial records, business strategies and intellectual property from home networks, personal devices, cloud platforms and shared workspaces. This has expanded the point at which confidential information is accessed and has made traditional approaches to confidentiality complex in practice.

The legal obligation of confidentiality remains unchanged. Businesses must therefore ensure that their Non-Disclosure Agreements (NDAs) address the realities of remote working and are supported by appropriate measures to protect confidential information. This article examines the legal basis of confidentiality in Kenya and the key considerations for protecting confidential information in a remote working environment.

1. THE LEGAL BASIS FOR CONFIDENTIALITY

The [Employment Act, 2007](#) does not impose a standalone statutory duty of confidentiality on employees. In Kenya, confidentiality obligations principally arise from the employment contract and the common law duties of fidelity, good faith and confidence. In [Leland I. Salano v Intercontinental Hotel \[2013\] eKLR](#), the Court recognised that an employment relationship is grounded in mutual trust, confidence, good faith and fidelity. The Court further held that the obligation to protect confidential information does not automatically end when employment terminates, although the post-employment obligation is narrower and is concerned with information that remains confidential or amounts to a trade secret.

An NDA therefore provides greater contractual certainty by identifying the information to be protected, regulating its use and disclosure and establishing continuing obligations after employment. It does not however convert every piece of information acquired during employment into protected information.

2. COMMON GAPS IN CONFIDENTIALITY ARRANGEMENTS

a. Defining confidential information

The starting point is to establish the confidential information to be protected. A definition that is too narrow may leave commercially sensitive information outside the scope of protection while one that is excessively broad may attempt to restrict an employee's use of general knowledge, skills and experience. The definition should therefore identify the categories of information that the business has a legitimate interest in protecting and distinguish them from information that an employee is entitled to retain as part of their professional knowledge and experience.

b. Authorised disclosure and third-party access

Employees may need to share confidential information with consultants, contractors, professional advisers and service providers. Confidentiality arrangements should therefore identify when disclosure is permitted and require third parties to maintain appropriate confidentiality safeguards.

Where personal data is involved, section 42 of the [Data Protection Act, 2019](#) requires controllers engaging processors to ensure that the processors provide adequate safeguards and to have a written processing agreement in place. [The Data Protection \(General\) Regulations, 2021](#) require these agreements

to address confidentiality, security, deletion or return of personal data and third-party access.

c. Access, storage and use in a remote environment

Remote working involves access to confidential information through personal devices, home networks, cloud storage and collaboration platforms. Confidentiality arrangements should therefore be supported by information-security measures governing access, downloading, copying, transferring and storing information.

Where personal data is involved, the Data Protection Act, 2019 requires appropriate technical and organisational measures to protect the data against unauthorised access, loss or disclosure. Employers should also ensure that any monitoring of employee devices, systems or communications is lawful, necessary and proportionate, particularly where personal devices are used.

d. Managing access at the end of employment

Confidentiality arrangements should also address the end of an employee's access to company information. In a remote working environment, confidential information may remain on personal devices, cloud accounts or downloaded files after employment ends.

Employers should therefore have procedures for withdrawing system access, recovering company devices and requiring the return or secure deletion of confidential information. Where personal data is involved, retention and deletion should comply with the applicable data protection requirements, including the obligation to retain personal data only for as long as necessary for the purpose for which it was collected.

3. RESPONDING TO A CONFIDENTIALITY BREACH

An NDA establishes contractual obligations concerning the use and disclosure of confidential information but it does not control how that information is technically accessed, stored or transmitted. Employers should therefore support contractual confidentiality obligations with appropriate information-security and remote-working measures. These may include role-based access, multi-factor authentication, encryption, secure cloud storage, restrictions on downloading or transferring information, and procedures for the use of personal devices and accounts.

Where personal data is involved, the Data Protection Act, 2019 requires appropriate technical and organisational measures to protect it. The Data Protection (General) Regulations, 2021 further require measures addressing information security, authorised access, secure storage and transfers, audit trails, event monitoring and breach management.

An effective confidentiality framework therefore combines contractual obligations with appropriate controls over how information is accessed and handled throughout the employment relationship.

4. RECOMMENDED APPROACH

Businesses should ensure that their contractual confidentiality obligations are supported by appropriate operational measures. We recommend:

- defining confidential information with sufficient precision to protect legitimate business interests without unnecessarily restricting employees' general knowledge and experience;
- identifying permitted disclosures and ensuring that consultants, contractors

and other third parties are subject to appropriate confidentiality and, where applicable, data processing obligations;

- implementing appropriate controls for remote access, personal devices, cloud storage and electronic communications;
- applying access controls based on employees' roles and responsibilities and reviewing access when roles change;
- establishing clear procedures for the return or deletion of confidential information and the withdrawal of system access when employment ends;
- ensuring that employee monitoring and security measures comply with applicable data protection requirements; and
- maintaining an incident-response procedure that enables suspected confidentiality and personal data breaches to be identified, contained and assessed promptly.

5. CONCLUSION

Remote work has changed how confidential information is accessed, used and stored. NDAs should therefore reflect these realities by defining confidential information, regulating its use and disclosure, and addressing obligations after employment ends.

Effective confidentiality protection requires contractual obligations to be supported by appropriate data protection, information-security and access controls. Businesses should therefore ensure that their NDAs remain aligned with how confidential information is actually handled in remote and hybrid working environments.

6. HOW WE CAN ASSIST

Our Employment and Labour Law team advises businesses on the contractual,

regulatory and operational aspects of protecting confidential information in the workplace. Our services include:

- Drafting and reviewing NDAs and confidentiality provisions in employment and commercial agreements;
- Reviewing employment contracts and remote-working policies;
- Advising on data protection obligations arising from employee and third-party access to information;
- Drafting and reviewing data processing and third-party confidentiality arrangements;
- Advising on employee exits and the protection of confidential information after termination;
- Advising on confidentiality and data protection issues arising from workplace investigations; and

- Advising on disputes involving the misuse or unauthorised disclosure of confidential information.

CM Advocates LLP advises employers and businesses on employment, commercial, technology and data protection matters, including contractual risk management, regulatory compliance and the protection of business information. For enquiries regarding this article or assistance with your organisation's confidentiality arrangements, please contact corporate.commercial@cmadvocates.com.

You may also visit [CM Advocates LLP](https://www.cmadvocates.com) for more information about our services.

Contributors:

Mercy Chore

Associate Advocate

mchore@cmadvocates.com

CM Advocates LLP – Contact Details

Head Office Nairobi

I&M Bank House, 7th Floor, 2nd Ngong Avenue

T: +254 20 2210978 or +254 716 209673

P.O. Box 22588 – 00505, Nairobi Kenya

E: law@cmadvocates.com

Mombasa Office

Links Plaza, 3rd Floor, Links Road, Nyali

T: +254 041 447 0758 / +254 41 447 0548

P.O. Box 90056 – 80100, Mombasa Kenya

E: mombasaoffice@cmadvocates.com

Regional Presence

Uganda | Tanzania | Rwanda | Zambia | Ethiopia | South Sudan

www.cmadvocates.com