

## PROPRIETARY INFORMATION AND CONFIDENTIALITY POLICY

## 1. Introduction

In the course of employment with RA, employees will be exposed to the company's Confidential Information. Confidential information is defined as confidential and proprietary information of the company to which the general public does not have access.

## 2. Confidential Information

This will include information about internal company matters or information which RA claims is confidential information and knowledge pertaining to products, designs, ideas, plans, trade secrets, proprietary information, sales and profit figures, customer and client lists, execution methodologies, confidential information received from customers, suppliers, agents, principals, partners, co-ventures, and other parties contracting with RA and its affiliates, and relationships with agents, representatives, customers, clients, suppliers, and others with whom RA or its affiliates have had or will have business dealings, accounts, systems, procedures, policies, strategies, research, business plans, financial data, contracts, price lists, formulas, techniques, technology, confidential reports, computer software, telephone lists, contract forms, files and all other information, knowledge, or data of any kind or nature relating to the products, services, or business of RA.

## 3. Procedure

The Employee will not during the employment or afterwards (except with the prior written consent of RA or as required by law) directly or indirectly:

- 3.1 Divulge or communicate to any person (including any representative of the press or broadcasting or other media) or through any social media any Confidential Information;
- 3.2 Cause or facilitate any unauthorized disclosure of any Confidential Information; or
- 3.3 Make use of (other than the benefits of RA) any Confidential Information.

The Employee shall use the best endeavors to prevent the unauthorized publication, disclosure or use of Confidential Information, including but not limited to business plans, services and products.

The Employee shall not without the prior written permission of RA except in the performance of his/her duties during the employment remove from RA premises any document, computer media or other tangible item which contain Confidential information, or which belongs to RA, its subsidiaries, its shareholders or its clients/customers, affiliates, suppliers or agents.

The Employee shall not without the prior written authorization of RA publish literature, deliver any lecture or make any recording, broadcast or demonstration relating in any way to RA activities or in which the name of RA is mentioned, except with the prior consent of RA or as required by law.

## 4. Financial Information

No employee shall release Financial Information if not approved by the CEO or CFO. Such requests could come in any form and may originate from existing or potential suppliers, customers, credit agencies, financial institutions, regulators, or other individuals or companies. Specific examples include:

- 4.1 A credit agency requesting a copy of RA's group financial statements via email;
- 4.2 A supplier requesting, we complete a financial disclosure form which details RA's annual sales and purchasing volumes; or
- 4.3 An employee of a customer asking you the value of RA's monthly billings.

If you receive a request to distribute Financial Information (either orally or in written form) you must notify the head of finance department immediately who will pass associated information to the CEO or CFO.

Additionally, as a company listed on the AIM Stock Exchange, all RA employees and certain third parties must ensure that they are aware of and adhere to the guideline as outlined in the "Groupwide Dealing Policy".

## 5. Summary

Confidential and Proprietary Information also includes any work product of the employee during his or her employment with the company including emails, reports, memorandums, research, and other similar documentation. Employees are prohibited from disclosing or duplicating such Confidential Information to non-employees except when there is a business need to do so. Upon termination of employment, the employee shall return all Confidential Information in the employee's possession. Employees are also prohibited from accessing files, databases, and other company resources which they do not have authorization to access.

Those found to be in violation of this policy will be subject to disciplinary action, up to and including termination. Violations may also result in legal action.



Soraya Narfeldt

CEO

Policy Implementation/ Review Date	Next Policy Review Date
January-2026	January-2027