

The logo consists of the letters 'SRM' in a bold, white, sans-serif font. A small orange triangle is positioned between the 'S' and the 'R'.

SRM

POLICY

# CODE OF CONDUCT

# TABLE OF CONTENTS

<b>Opening Statement</b>	<b>4</b>
 Clause	
1. Scope	5
2. Our values	5
3. Governance and responsibility for the code	5
4. Workplace environment	6
5. Business practices	7
6. Company assets and information	9
7. Your responsibilities	11
8. Non-retaliation	12
9. Consequences of failure to comply	12
10. Process for review	12

## Opening statement

Our culture here at S-RM is the result of years of talented, curious people coming together and working out how best to solve complex problems for our clients, and it's our ability to bring sharper thinking to everything we do which enables us to stand apart from the competition. Key to our success is our people and our unequivocal commitment to conducting our business ethically and in accordance with applicable laws and regulations. Many of our services are intrinsically linked to ethical business practices and support clients in achieving compliance with their legal and regulatory obligations by providing them with actionable information to make decisions.

S-RM's Supervisory Board and Executive Committee are committed to ensuring that our business has in place appropriate systems, policies, and processes to support and promote effective governance and ethical decision-making, reflective of the specific risks and nuances of the industry in which we operate. Our core values are based on transparency, collaboration and trust and it is on these foundations that we will continue to build our business and our brand.

The purpose of this Code of Conduct (the "Code") is to give guidance on ethical business practices and to have a clear set of standards and principles outlining how we are all expected to operate. Although much of the guidance is common sense, we require you to read the Code carefully and embed it in your everyday work. It is not intended to address every situation that may arise, and we therefore rely on you to exercise sound judgment and decision-making, seeking clarity where appropriate. If you have any questions about the Code or believe it has been violated, please do not hesitate to discuss with your manager, HR, the Legal, Risk & Compliance team or with me directly.

Thank you for committing to our Code of Conduct.

Yours sincerely,

**Heyrick Bond Gunning**  
Chief Executive Officer



## 1. Scope

**1.1** The Code applies to all persons working for S-RM Intelligence and Risk Consulting Limited or any group company ("**S-RM**" or the "**Company**"), including employees at all levels, directors, officers, agency workers, seconded workers, volunteers, interns, and individual temporary or fixed term contractors, wherever located. We also expect our subcontractors, consultants, vendors, and partners to comply with the principles of the Code and our core values when working for or on behalf of S-RM.

**1.2** The Code does not form part of any contract of employment or contract to provide services and we may amend it at any time.

**1.3** All policies, procedures and guidelines referenced in this Code are available on the Company's intranet.

## 2. Values

**2.1** Our commitment to conduct our business and relationships with transparency and the highest standard of ethical conduct is consistent with S-RM's four core values which are:

- We put client service at the heart of everything we do
- We trust, respect and look out for each other
- We are collegiate and put the team before ourselves
- We are always learning and sharing our knowledge

**2.2** We believe that embedding these values in our work and everyday practice helps us to maximise value when providing service to clients. In addition, these values help make S-RM an inclusive and supportive environment for our employees and one which fosters learning and development.

**2.3** Part of our bi-annual performance review includes appraising employees at all levels of the Company against how well we have demonstrated these values. This process ensures that each of us are held accountable and that these values become embedded in our company culture.

## 3. Governance and responsibility for the code

**3.1** Our corporate governance structure aims to promote responsible and ethical decision making which considers the interests of all stakeholders, including environmental and social factors in addition to the financial. We have several formal committees in place as part of this structure. They include the Board of Directors of the Company (the "Supervisory Board"), the Executive Committee, the Remuneration Committee, and the Risk Committee. Each Committee has a specific purpose and mandate. We seek to structure and organise our committees in a manner that ensures that they are attended by those with the necessary skills and expertise, so that independence and objectivity is preserved and that decisions are taken at the appropriate level.

**3.2** The Supervisory Board has ultimate responsibility for ensuring that the Code complies with our legal and ethical obligations, and that all those under our control comply with it. The Executive Committee has primary and day-to-day responsibility for implementing the Code.

**3.3** In adopting the Code, the Supervisory Board and Executive Committee acknowledge that implementation of its provisions is a core accountability of the Executive Committee, but they are also subject to and responsible for complying with the Code.

**3.4** The Supervisory Board and Executive Committee recognise the importance of separating corporate governance, assurance, and management of governance-related risk from the executive management of the Company, hence, the S-RM Risk & Compliance and Legal teams are

responsible for monitoring the Code's use and effectiveness, dealing with any queries relating to its content, auditing internal control systems and procedures to ensure they are effective in managing ethics and conduct on behalf of S-RM, and providing adequate and regular training on the Code and the issues covered by it.

**3.5** S-RM operates an Enterprise Risk Management (ERM) Framework, which includes assessing and managing risks associated to our business conduct and ethics, such as modern slavery and human trafficking. The S-RM Risk Management Procedure provides guidance on how we assess and respond to risk across the business, including all S-RM business units, departments, and international offices. The S-RM Risk Committee has responsibility for and oversight of these processes and meets on a quarterly basis to review their effectiveness.

**3.6** Management at all levels are responsible for ensuring those reporting to them understand and comply with the Code.

## 4. Workplace environment

### 4.1 Equality, Diversity and Inclusion

We firmly believe that equality, diversity, and inclusion (EDI) is critical for our business to continue to evolve, to enhance our culture and brand, and to allow us to achieve our strategic aims. The diversity of skills, backgrounds and experiences at S-RM enables us to respond to our clients more effectively. Our EDI Lead holds a strategic leadership role in helping us continually improve EDI at S-RM. Working within the People Practice and chairing our EDI Council, they are integral to our agenda in this area. The EDI Council meets regularly to discuss how to profile and highlight issues of interest and concern throughout S-RM. Alongside the EDI Lead, council members, champions and employee network groups engage throughout the business to understand our colleagues' views on equality, diversity and inclusion at S-RM. More

details and further information is available on the Company's intranet.

### 4.2 Discrimination, Harassment and Bullying

We are committed to providing an inclusive work environment recognised for its equality and diversity, and we treat everyone with fairness, respect and dignity. We do not tolerate any discrimination. Discrimination includes all unequal treatment, exclusion or preference based on race, gender, age, disability, sexual orientation, religion, political views, national or ethnic origin or any other characteristic that results in compromising the principle of equality. We expect you to demonstrate professionalism and integrity at all times and to treat everyone you meet through work or work-related activities in a respectful manner. We will not tolerate any form of harassment or actions that reasonably can be considered as offensive or intimidating, including any form of unwanted attention of a sexual nature. As part of your contract of employment you are expected to familiarise yourself with our internal HR policies and employee handbook upon joining the business, this includes the **S-RM Dignity at Work Policy**.

### 4.3 Health, Safety and Wellbeing

We are committed to providing a safe and healthy work environment for employees, clients, and visitors whether working in or visiting an S-RM office, travelling for business or working remotely. We have controls, training and resources in place which aim to ensure prevention of accidents and promote a safe and healthy working environment. We maintain the **S-RM Health and Safety Policy** and the **S-RM Travel Policy**, which provide more detail on both topics. We provide information about workplace safety and health issues through internal communication channels such as manager-employee meetings, intranet postings, memos, or other communications. You must immediately report any unsafe condition to your manager or the relevant office manager.



#### 4.4 Workplace Violence

We will not tolerate any acts or threats of violence against our employees, clients, vendors, subcontractors, or visitors either on Company premises or through its communications channels. Additionally, any acts or threats of violence committed by employees or sub-contractors while doing business on behalf of the Company will not be tolerated. Any threatening behaviour must be reported immediately.

#### 4.5 Drugs and Alcohol

Using, consuming or being under the influence of drugs, alcohol, or any other substance that may impair your ability to work safely and productively is strictly prohibited. No employee or other personnel may sell, buy, use, possess, or transfer illegal drugs or other illegal controlled substances while on Company premises or while conducting Company business. Drinking or being under the influence of alcohol in the workplace or while conducting Company business is also prohibited, except for moderate and responsible consumption of alcohol in appropriate firm-sanctioned events or business-related entertainment functions.

### 5. Business practices

#### 5.1 Conflicts of Interest

A conflict of interest may occur when your personal interests and S-RM's interests are different and this may interfere with your ability to perform your work objectively and effectively. We expect you to always act in the best interests of S-RM when you are representing the Company. You should also avoid situations that could be perceived as a conflict of interest. Conflicts may arise, for example, from personal investments or financial interests, service on boards of other entities, outside employment, personal or family relationships that overlap with your professional life, financial or business relationships, or any situation in which you may be inappropriately influenced in making a business decision. As it is not possible to describe every potential conflict

of interest, we rely on you to exercise sound judgment, seek advice when appropriate, and avoid situations where anyone could question whether you were inappropriately influenced in making a business decision. You must disclose to the Risk & Compliance team any activities that you think might involve a conflict of interest.

We have in place well established processes and procedures which seek to avoid any conflicts of interests arising either at the outset of or during a client engagement. Any actual or potential conflicts are flagged and escalated immediately for resolution. We also conduct compliance checks on all clients as part of the onboarding process.

#### 5.2 Competition

S-RM conducts its business in accordance with all applicable competition laws (also referred to as antitrust laws in some jurisdictions). In general, these laws prohibit unfair methods of competition and activities designed to unreasonably restrain trade. Failure to comply with applicable antitrust or competition laws can result in custodial sentences for individuals and large monetary penalties for both the Company and individuals. Additionally, in some jurisdictions private parties may bring civil suits to recover damages. Competition laws prohibit agreements or understandings among competitors that are deemed collusive or anti-competitive, such as agreements to fix prices, restrict output or sales, reduce or eliminate competition in a competitive bidding process, or similar practices. Competition laws may also prohibit discrimination in pricing, terms, and services among clients, exclusive dealing agreements whereby one party only does business with another party if they agree to deal with them exclusively, tying arrangements where a client is required, as a condition of purchasing one product, also to purchase a second, distinct product, and "predatory pricing" where a company offers a sales price below a product's cost to drive competitors out of the market. You must refrain from any activity associated with price fixing, bid rigging, and other anti-competitive actions. You should inform the Legal or Risk & Compliance teams immediately of possible violations of fair competition practices of which you become aware. Company business. Drinking or

being under the influence of alcohol in the workplace or while conducting Company business is also prohibited, except for moderate and responsible consumption of alcohol in appropriate firm-sanctioned events or business-related entertainment functions.

### 5.3 Bribery and Corruption

We have a zero-tolerance policy towards bribery and corruption and have in place strict controls to prevent the occurrence of bribery or corruption within our business. We comply with all applicable anti-corruption laws and regulations and ensure that business activity is conducted in a fair and transparent manner. The **S-RM Anti-bribery and Corruption Policy** is available on the Company's intranet and includes guidance on the receiving and giving of gifts and hospitality and in relation to managing potential risks associated with tax evasion. We also require all employees to complete anti-bribery and corruption training.

### 5.4 Gifts and Hospitality

Offering or accepting gifts or entertainment may be appropriate and permissible as part of the normal business process to the extent it does not influence or appear to influence business decisions. We must never accept gifts or other benefits if our business judgment or decisions could be affected. Offering or accepting any gift or entertainment must be in compliance with applicable laws and regulations, this Code and Company policies. Please refer to the guidance on the giving of Gifts and Hospitality in the **S-RM Anti-bribery and Corruption Policy** for more information.

### 5.5 Anti-money Laundering

Money laundering is the process of disguising the proceeds of crime in order to hide its illegal origins or otherwise dealing with the proceeds of crime. Criminal proceeds include not only money, but all forms of assets, real estate, and intangible property that are derived from criminal activity. Money laundering is illegal and supports other criminal activities, including drug

trafficking, terrorism, corruption, human rights violations and tax evasion. Tax evasion is an illegal practice where a person or entity evades paying their actual tax liability. S-RM complies with all applicable anti-money laundering laws. We do not tolerate the facilitation of tax evasion by persons who act for or on behalf of S-RM. You each have a duty to act diligently to prevent our services from being used to further money laundering and terrorist financing. You must know and understand the clients you are dealing with and obtain the necessary information and undertake KYC (know your customer) checks to verify the identity of each client. We only conduct business with clients willing to provide us with information regarding their true identity and ownership structure. We avoid the transfer of funds to or from entities or countries not related to a transaction, for example, we cannot accept payment from third parties. You are reminded to be attentive to unusual payments, invoicing, and banking arrangements as well as unusual tax status of suppliers. You must be vigilant of any suspicious activity and immediately report any concerns to the Risk & Compliance, Finance or Legal teams.

### 5.6 Trade Sanctions

We have implemented strict processes to ensure that we comply with all applicable economic and trade sanctions imposed against countries, governments, individuals, and entities specified by the competent authorities in the jurisdictions where we conduct business. We will not deal, directly or indirectly, with any person, entity, or group subject to antiterrorism measures or whom we believe or have reason to believe is involved in the financing of terrorist activities. We expect you and our subcontractors to comply at all times with the processes that we have put in place to manage sanctions related risk and to comply with any other sanctions or trade restrictions that apply to you individually within your country of residence or operations. You should seek advice immediately from the Legal team if asked to deal with a sanctioned party, market or country.

### 5.7 Client and Engagement Intake

We recognise that some clients, particularly those in controversial industries or in certain jurisdictions may present certain risks for the Company. We have in place a process for identifying and reviewing clients and engagements to ensure that S-RM's provision of services and client base is consistent with our internal ethics and core values including but not limited to the principles of the Code.

### 5.8 Third Party Management

We work with a range of third parties, including subcontractors, consultants, vendors, and suppliers in the course of business. Before engaging with any third party, you must follow our internal procedures to ensure the relevant risk assessment and due diligence has been completed. Any suppliers or vendors having access to confidential information must complete an information security assessment and be approved by our Information Security Team. All third parties must be onboarded in accordance with the **S-RM Subcontractor Onboarding Procedure** and the **S-RM Supplier Onboarding Procedure** which includes stringent vetting that is completed during initial onboarding. Our standard Subcontractor Agreement contains robust provisions addressing confidentiality, conflicts and standard of services and requires the subcontractor to comply with all applicable laws, including applicable anti-corruption and modern slavery laws, and with this Code. If you are engaging a third party, you are responsible for ensuring that the third party understands our core values and the Code and conducts themselves in accordance with its principles at all times whilst working for us. Any concerns relating to any third parties working for us should be immediately raised with your manager and the Risk & Compliance team.

### 5.9 Slavery, Human Trafficking and Child Labour

We are committed to upholding human rights in all our operations, and we oppose the use of modern slavery in all forms. Various laws prohibit trafficking in persons, including trafficking-related activities. S-RM has a

zero-tolerance policy for participating in or benefitting from any form of human trafficking or modern slavery, forced or involuntary labour, or child labour under any circumstances. We comply with all applicable laws and regulations relating to minimum wage, working hours, overtime pay, and age of our employees. Furthermore, we will not do business with any third parties or suppliers who do not operate in compliance with human rights laws. You must immediately report any human rights violations observed within S-RM or committed by our suppliers or third parties. See the **S-RM Modern Slavery Statement**.

## 6. Company assets and information

### 6.1 Intellectual Property

Intellectual property rights in S-RM's proprietary tools and platforms and in the services and deliverables we provide are a critical asset of the business. Unauthorised use can lead to their impairment or serious loss of value. You are required to protect and preserve all Company's intellectual property and take all steps required to ensure that all such rights vest in the Company. All employees are also required to ensure they do not infringe any third party intellectual property rights, including laws governing the fair use of copyrights, trademarks, brands, and licensing agreements. Any suspected misuse of trademarks, logos, or other intellectual property should be immediately reported to Legal or the Risk & Compliance team. Please also refer to the **Third Party Use of S-RM Logo guidelines** available on the Company's intranet.

### 6.2 Assets

The Company requires all employees to protect its assets. Assets include facilities, equipment, computers and information systems, telephones, employee time, confidential and proprietary information, corporate opportunities and Company funds. All assets should be used for legitimate purposes, efficiently, and for Company business only. Suspected incidents of



fraud, theft, negligence, and waste should be reported to a member of the Executive Committee.

### 6.3 Confidential Information

Due to the nature of our business, confidentiality and security of confidential information is of paramount importance and all employees and subcontractors are subject to legal and contractual duties to keep confidential all S-RM and client information and to protect it against unauthorised loss, access, or disclosure.

You may only access confidential information when access is both authorised and necessary for the performance of job duties and must not disclose confidential information to any person who does not have permission to receive it. You should only share confidential information with other S-RM employees where there is a legitimate business reason to do so and must not disclose confidential information outside of the Company, except where authorised in writing to do so by the Company or client or such disclosure is essential to the performance of job duties. Where disclosure is permitted, a non-disclosure, confidentiality or other agreement may be required prior to such disclosure. You must only use approved Company systems to store, manage, and transmit confidential information. Your confidentiality obligations survive termination of your employment or engagement indefinitely. You must not disclose confidential information to a new employer, and you may not disclose your previous employer's confidential information to us.

### 6.4 Material Non-Public Information

In the conduct of normal business, you may become aware of or come into possession of information that is not in the public domain and which, if released into the public domain, might have a significant impact on the price of tradeable securities. These securities are typically those issued by either subjects of S-RM work or S-RM's clients but may also relate to other issuers. The misuse of this material non-public information (MNPI) is a criminal

offence in all of the jurisdictions in which S-RM employees are located. Risks exist for (i) individual employees, should they wittingly or unwittingly trade on the basis of MNPI for their own or someone else's account, or induce someone else to trade on the basis of the same; (ii) for S-RM, should the Company, its employees or processes be implicated in the mishandling of MNPI; (iii) for S-RM's clients should they receive MNPI from S-RM, since this may, for example, compromise their own internal investment or commercial business processes; (iv) S-RM's subcontractors, should they be placed in a situation where in the course of conducting work for S-RM they have come into possession of and/or act – knowingly or unknowingly - on MNPI. You are required to complete training annually in order to (i) be equipped to identify MNPI, (ii) be aware of the risks of misusing MNPI and how to mitigate them, (iii) understand escalation procedures in the event of coming into possession of MNPI or being uncertain about whether or not something may be MNPI, (iv) understand, agree, and adhere to the firm's policies around the ownership and trading of securities in situations relating to MNPI.

### 6.5 Data Protection and Security

In the normal course of our business, we collect personal data about individuals, including employees, clients, suppliers, and other persons with whom we or our clients do business. The Company is committed to complying with applicable data protection and privacy laws in all jurisdictions in which we operate. We have in place the following policies which govern our compliance with applicable data protection and privacy laws: **S-RM Data Protection Policy, S-RM Data Retention Policy, S-RM Data Classification Policy, and S-RM Data Subject Access Requests Procedure**. We routinely update the **S-RM Privacy Policy** to detail how we process personal data and the lawful basis on which we rely.

We have appointed a Data Protection Officer to oversee our data protection compliance. We have a documented S-RM Information Security Policy in place to ensure that information is protected from loss of confidentiality, integrity, and availability. We have a dedicated in-house

Information Security team in place who deploy technical controls and testing to mitigate against cyber risk. We require you (and subcontractors with access to S-RM systems including email) to complete information security training and adhere to all information security policies. You should familiarise yourselves with all information security related policies available on the Company's intranet.

### 6.6 Records

S-RM is committed to maintaining records needed to meet our legal, regulatory, tax and accounting obligations and to deleting records when no longer required, in compliance with all applicable laws. You must follow the **S-RM Data Classification and Data Retention Policies**. If you become aware of actual or potential claim, litigation or government investigation, you should immediately contact the Legal team. You must retain and preserve all records from destruction that may be relevant to the matter until you are advised how to proceed by the Legal team.

### 6.7 Use of Information and Communication Systems

All employees and subcontractors must comply with the **S-RM Acceptable Use Policy** when using any company communication systems.

### 6.8 External Communications

You are not permitted to make any statements to the press or to accept any public speaking engagements without prior approval from the Marketing team. Whilst we encourage you to promote the Company on social media such as LinkedIn, you should ensure that any external communications (including online and social media posts) are appropriate and well judged, do not disclose confidential proprietary information, and do not give the impression that you are speaking on behalf of the Company unless authorised to do so. Please refer to the **S-RM Media Engagement Policy** and **S-RM Social Media Guidelines** available on the Company's intranet.

### 6.9 Charitable Donations and Volunteering

S-RM's Corporate Social Responsibility (CSR) agenda is guided by S-RM's core values. We aim to unite colleagues in 'giving back' and making positive environmental and social impacts through their work. These efforts are overseen by S-RM's local CSR Committees and a member of the Executive Committee. As part of this, we periodically make donations to appropriate approved charities and causes (all donations must be approved by the responsible Executive Committee member). We also give all employees one day of paid leave each year to participate in a volunteering initiative, which is approved by the relevant line manager and recorded on our human resource system. For further information on our CSR programme, please refer to the **S-RM Corporate Social Responsibility Principles** and **S-RM Employee Volunteering Policy**, both of which can be found on the CSR area of the Company's intranet.

### 6.10 Environmental Action and Sustainability

We recognise the vital part that businesses have to play in increasing sustainability and protecting the environment and are committed to continual improvement on both fronts. We already track our carbon emissions as part of our ISO 14001 (Environmental Management) certification and offset our carbon footprint that arises from our corporate business travel through our work with our CSR partners, which may include charities and other not-for-profit organisations. We actively engage with our employees on issues relating to the environment, encouraging and supporting them to put 'green practices' into place both at work and home. For example, we promote sustainable transport initiatives such as 'cycle to work' schemes, subject to availability in each of our office locations. The **S-RM Environmental Policy** is available on the S-RM website.

## 7. Your responsibilities

7.1 You must ensure that you read, understand and comply with the Code.

**7.2** You must also:

Notify your manager or the Legal, Risk & Compliance team as soon as possible if you believe or suspect that a breach of the Code has occurred or may occur in the future;

- Co-operate with any investigation that S-RM undertakes;
- Understand and comply with specific laws and regulations that apply to your specific role; and
- Complete any mandatory associated training that is offered to you.

**8. Non-retaliation**

S-RM strictly prohibits retaliation against any person for making a good faith report of suspected misconduct, raising concerns, asking questions about the Code, or cooperating in an investigation. If you report a suspected breach and it turns out that a breach has not occurred, you will not be penalised for reporting in good faith if you came forward with information you believed to be true. Retaliation is a serious contravention of the Code and anyone engaging in acts of retaliation will be subject to disciplinary action. Anyone making a report in bad faith may also be subject to disciplinary action.

**9. Consequences of failure to comply**

Disciplinary action, up to and including termination and/or legal proceedings, may result from any failure to comply with the Code, applicable laws, rules or regulations and any other S-RM policy or procedure.

**10. Process for review**

10.1 The Code will be reviewed annually or as required following any legislative changes that might impact on it, any changes to other associated internal policies, processes or procedures or any breach or other incident relating to the issues addressed in the Code.





# S-RM is a global intelligence and cyber security consultancy

We support our clients by providing intelligence that informs critical decision-making and strategies, from investments and partnerships through to disputes; by helping organisations build resilience to cyber security threats; and by responding to cyber attacks and organisational crises.

## —— For more information

Visit our website at [www.s-rminform.com](http://www.s-rminform.com)

Email us at [hello@s-rminform.com](mailto:hello@s-rminform.com)

CONNECT WITH US ON SOCIAL MEDIA

