Discovery

JULY

2026

Anti-Financial Crime Policy Statement

Including anti-money laundering, counter-terrorist financing, counter-proliferation financing, anti-bribery and corruption and sanctions compliance

1. PURPOSE

This Anti-Financial Crime Policy Statement ('Policy Statement') sets out the framework used by Discovery Limited and its subsidiaries ('Discovery' or 'the Group') for preventing, detecting and responding to financial crime across its operations ('Anti-Financial Crime Framework'). The Group is committed to combating financial crime by adhering to all applicable local and international laws, regulations, industry standards and best practices, while upholding the highest ethical and professional standards and its core values.

Operating across multiple jurisdictions, including South Africa, the United Kingdom and the United States of America, Discovery recognises its responsibility as a regulated and responsible corporate citizen to maintain robust and effective financial crime controls. The Group adopts a zero-tolerance approach to financial crime and is committed to ensuring that money laundering, terrorist financing, proliferation financing, corruption, bribery and the granting or acceptance of improper advantages (collectively 'financial crimes') have no place within its operations.

A strong financial crime compliance culture is fundamental to maintaining trust, protecting the Group's reputation, safeguarding its assets and stakeholders, and supporting sustainable and responsible growth.

2. SCOPE

The Anti-Financial Crime Framework applies to Discovery and all its South African and international subsidiaries, including:

1. All executive and non-executive directors
2. Full-time, part-time and temporary employees
3. Any independent contractors, consultants under Discovery's direct control and third parties acting on Discovery's behalf.

The Group seeks to encourage business partners to act in line with its values and the principles of its Anti-Financial Crime Framework, including where it does not exercise direct control or operational authority. Business partners are defined as any third party with whom the Group has an existing business relationship, is considering entering such a relationship, or is in the process of finalising one. This expectation is reinforced through contractual provisions, including clauses related to financial crime compliance, which serve to uphold the Group's standards and mitigate associated risks.

3. IMPLEMENTATION

Discovery requires that each entity within the Group:

1. **Follow applicable legislation:** Adhere to relevant anti-money laundering, counter-terrorist financing, counter-proliferation financing (AML, CTF and CPF), anti-bribery and corruption (ABC) and sanctions laws in their respective jurisdictions.
2. **Develop consistent policies**: Entities must develop consistent policies in relation to financial crime but may create their own policies if they align with each of the financial crime policies (whether specific to AML, CTF, CPF, ABC, sanctions or the collective).
3. **Align operations:** Implement procedures consistent with the spirit of each financial crime policy (whether specific to AML, CTF, CPF, ABC, sanctions or the collective).
4. **Monitor compliance** with the financial crime policies.
5. **Implement training**: Each directly held intermediate holding company of Discovery Limited, or the CEO of the Discovery entity, as relevant and applicable, is responsible for ensuring that appropriate training and awareness programmes are rolled out. The nature and complexity of roles in the entities determine the content of these programmes. Employees must complete mandatory training.

Each directly held intermediate holding company of Discovery Limited must oversee the adherence to financial crime policies by the boards of its directly or indirectly held subsidiaries. Other than where a dedicated intermediate holding company exists, for the South African domiciled subsidiaries that are directly held by Discovery Limited, the Chief Executive Officer of the South African composite (CEO of SA Inc) fulfils the oversight role and other responsibilities of directly held intermediate holding companies as set out in the financial crime policies.

4. POLICIES

Discovery has established the following policies that outline the Group's approach to ensuring full compliance with all relevant and applicable financial crime laws in their respective jurisdictions:

Policy	Approval	Review frequency
Group-wide Anti-Bribery and Corruption (ABC) Policy	▪ Discovery Limited Risk and Compliance Committee ▪ Discovery Group Executive Committee	Every two years or out of cycle due to an operational or regulatory trigger event
Group-wide Sanctions Policy	▪ Discovery Limited Risk and Compliance Committee ▪ Discovery Group Executive Committee	Every two years or out of cycle due to an operational or regulatory trigger event

Policy	Approval	Review frequency
Anti-Money Laundering, Counter-Terrorist Financing and Counter-Proliferation Financing Risk Management and Compliance Programme (RMCP)	▪ Discovery SA Composite Risk and Compliance Committee ▪ Discovery SA Executive Committee	Yearly or out of cycle due to an operational or regulatory trigger event
Group Financial Crime Risk Management Policy	▪ Discovery Limited Risk and Compliance Committee ▪ Discovery Group Executive Committee	Every three years or out of cycle considering emerging risks, or operational or regulatory trigger events
Vitality Financial Crime Policy	▪ UK Policy Sub-committee	Yearly or out of cycle due to operational or regulatory trigger events

4.1 GROUP-WIDE ABC POLICY

INTRODUCTION

Discovery's Group-wide Anti-Bribery and Corruption (ABC) Policy sets out a comprehensive framework to prevent, detect and manage bribery and corruption risks across the Group. It establishes a zero-tolerance approach to all forms of bribery and corruption, applies to both public and private sector interactions, and defines prohibited conduct broadly, including monetary and non-monetary inducements.

The ABC Policy outlines expected standards of acceptable behaviour, emphasising transparency, adherence to established procedures, refusal of improper advantages, robust due diligence on business partners and suppliers, and timely reporting of concerns. It further provides clear guidance on high-risk areas such as gifts and entertainment, political contributions, sponsorships, charitable donations and facilitation payments, all of which are subject to strict controls and disclosure requirements.

BRIBERY AND CORRUPTION

Discovery strictly prohibits paying bribes, categorically rejects all forms of bribery and corruption, and is committed to acceptable behaviour.

A bribe is an inducement or reward offered, promised or provided to gain any commercial, contractual, regulatory or personal advantage. A bribe could be a financial or other advantage, with the intention that a 'relevant function or activity' should be performed 'improperly' as a result.

A bribe may be monetary or non-monetary, tangible or intangible. A bribe may take the form of, or be facilitated through:

- Payments of money
- Gifts or entertainment
- Discounts, loans or financing given on non-commercial terms
- Rebates or kickbacks in relation to services provided
- Overpayments to business partners
- Use of assets at a discount or free of charge
- Sponsorships, charitable contributions and community investments

- Political contributions
- Employment or internships
- Information or assistance.

Corruption is defined as an act of accepting or offering any bribe or gratification from any other person, whether for the benefit of that person or any other person, to influence the other person to act in a manner that is illegal, dishonest, unauthorised, incomplete, biased or in a manner that results in the misuse or selling of information.

Both bribery and corruption apply to private and public individuals, encompassing the offering and acceptance of bribes, regardless of the individuals involved.

In the context of anti-bribery and corruption, 'acceptable behaviour' means engaging in business practices with full transparency, adhering to established protocols, rejecting any offer or acceptance of bribes or improper advantages and swiftly reporting any suspicious actions. It emphasises prioritising ethical conduct over personal gains.

We apply the following key aspects of acceptable behaviour in anti-bribery and corruption practices:

- **Transparency in transactions:** We clearly document all business dealings, including interactions with government officials, and ensure all payments are made through legitimate channels.
- **Following established procedures:** We adhere to Discovery policies and legal guidelines regarding gifts, donations and interactions with third parties.
- **Refusing bribes:** We never offer, accept or solicit bribes in any form, whether monetary, gifts or favours, to influence business decisions.
- **Due diligence on business partners and suppliers:** We conduct thorough background checks on suppliers and potential business partners to assess their compliance with anti-bribery laws.
- **Reporting concerns:** We encourage any person to report any suspected bribery or corruption without fear of retaliation through established internal reporting mechanisms.
- **Fair competition:** We engage fairly in competitive bidding processes without attempting to manipulate the outcome through improper means.
- **Gift giving with caution:** If gift giving is appropriate, measures are taken to ensure that gifts are modest and are not construed as intending to influence business decisions. All gifts must be properly disclosed.
- **We do not tolerate unacceptable behaviour, including:**
  - Offering or accepting large gifts or favours to secure a business deal
  - Making payments to facilitate a process without proper documentation
  - Using intermediaries to funnel bribes
  - Making false or misleading statements on official documents
  - Pressuring others to engage in corrupt activities.

GIFTS AND ENTERTAINMENT

Proper management of gifts and entertainment is crucial to avoid actual and perceived bribery or corruption. Discovery has a documented policy that all employees are subject to, which requires disclosure of gifts given and received. Discovery conducts risk-based due diligence before engaging in sponsorships, charitable contributions or community investments.

POLITICAL FUNDING

Discovery does not seek to influence the political process through improper means. Contributions to political campaigns, parties, candidates or politically affiliated organisations strictly adhere to our Group Political Funding Policy.

BUSINESS PARTNERS AND SUPPLIERS

Discovery expects its business partners and suppliers to share Discovery's commitment to ethical and responsible business practices. The Group seeks to encourage business partners and suppliers to act in line with its values and the principles of its Anti-Financial Crime Framework, including where it does not exercise direct control or operational authority. To manage bribery and corruption exposure associated with business partners and suppliers, Discovery implements a range of controls and processes, including screening, due diligence and monitoring, using a risk-based approach. Discovery endeavours to conduct a due diligence assessment using a risk-based approach before entering into business partnerships, enabling Discovery to identify, assess and mitigate any risk of corruption posed by the partnerships. Discovery entrenches appropriate compulsory anti-corruption and bribery clauses in all contractual arrangements. Where appropriate, Discovery also conducts ongoing monitoring.

FACILITATION PAYMENTS

In certain jurisdictions, public officials may request small payments, known as facilitation payments, to expedite routine governmental actions (for example, issuing permits or licences). Facilitation payments constitute bribery. Discovery never pays or authorises such payments. Requests for facilitation payments must be promptly reported to the relevant Compliance function.

ACCURATE RECORD-KEEPING AND FINANCIAL ACCOUNTING

Discovery ensures all transactions are accurately recorded in a manner that reflects their nature and substance. This is done in accordance with Discovery's approved and documented procedures, which align with global best practices and standards.

REPORTING AND WHISTLEBLOWING

The Group expects and encourages its clients, directors, employees, suppliers, business partners and contractors to speak openly and raise concerns about possible non-compliance through the available reporting channels, or with a manager or supervisor where applicable. Discovery takes all concerns seriously and endeavours to address them as promptly as possible.

There are various avenues available to report a concern (as set out in the Whistleblowing Policy), including the following:

South Africa	▪ Discovery Group Whistleblowing Hotline toll-free phone: 0800 00 45 00 ▪ Email: discoveryforensics@whistleblowing.co.za or discoveryethics@whistleblowing.co.za ▪ The Financial Crime Compliance Unit at Suspicious_Transactions@discovery.co.za
United Kingdom	▪ Anonymous Whistleblowing Hotline toll-free phone: 0800 333 362

	▪ Email: whistleblowing@vitality.co.uk
United States of America	▪ Email: Whistleblowing_VGI@Vitalitygroup.com

ADHERENCE, INCIDENT INVESTIGATION AND CORRECTIVE ACTIONS

Our policies support Discovery's values and reflect what is important to us. We take breaches of our policies seriously. Depending on the severity of the breach, consequences for employees may range from a warning to the termination of employment. All instances of non-compliance with any anti-financial crime-related policy or process will be included in regular risk and compliance reporting and reported to the relevant board committee and to law enforcement or regulatory authorities, as prescribed.

DUTY TO PREVENT CORRUPT ACTIVITIES AND BRIBERY ACTIVITIES

Offences relating to the failure to prevent corrupt activities are part of anti-bribery and corruption regimes globally. Discovery is committed to fully complying with the anti-corruption requirements of the jurisdictions in which it operates. This includes aligning with the 'Six Principles approach', which emphasises establishing robust anti-bribery and anti-corruption frameworks.

Discovery is dedicated to taking all reasonable steps to prevent corrupt activities within our operations and business relationships, to ensuring our policies, procedures and training reflect these principles, and to holding ourselves accountable for maintaining a culture of integrity and transparency in all business dealings by:

1. Implementing ABC policies and procedures that are proportionate to the risks faced by Discovery
2. Ensuring that senior management demonstrates a clear commitment to preventing bribery and corruption, setting the tone from the top
3. Conducting regular and thorough assessments to identify and understand the specific bribery and corruption risks the organisation faces
4. Performing due diligence on all parties involved in business transactions to mitigate bribery and corruption risks
5. Providing regular training and clear communication to all employees and stakeholders about Discovery's ABC policies and procedures
6. Continuously monitoring and reviewing ABC measures to ensure they are effective and making improvements as necessary.

4.2 GROUP-WIDE SANCTIONS POLICY

INTRODUCTION

Discovery's Group-wide Sanctions Policy establishes the framework for ensuring compliance with applicable international and domestic sanctions regimes across all jurisdictions in which the Group operates. It reflects the Group's commitment to responsible corporate conduct and recognises the significant regulatory and reputational risks associated with sanctions breaches.

The Group operates in multiple countries, including South Africa, the United Kingdom and the United States of America. As a responsible corporate citizen and a licensed regulated Group, we are committed to comply with sanctions regimes and the laws of the jurisdictions in which we operate. Upholding compliance with global sanctions is critical to protecting Discovery and its stakeholders.

The Group adheres to the following principles:

1. The Group will not engage in any business activity that would result in a breach of applicable sanctions legislation in any jurisdiction in which it operates. Where sanctions apply, the Group will forgo business opportunities in the affected jurisdiction to ensure full compliance with the relevant legal obligations. The Group may decide not to provide products or services even where it is permitted by law. These decisions may be guided by risk appetite, corporate social responsibility, business efficiency or reputational risk.
2. In carrying out its compliance obligations, the Group relies on information provided to it by its clients, employees and business partners, unless it is aware or suspects that those clients, employees and business partners, or the information provided, is unreliable or dishonest.
3. The Group reports any sanctions breaches to the appropriate authority in a timely manner and in accordance with law and applicable regulations.

The Group applies a risk-based approach in adhering to these principles. Therefore, the Group must assess and understand the sanctions risks posed by a client, employee or business partner and apply sanctions risk management measures appropriate to the level of risk.

MANAGING SANCTIONS RISK

To manage the Group's sanctions risk, Discovery implements a range of procedures and controls, including those related to dealings with clients, suppliers, business partners and record-keeping.

Sanctions screening
Sanctions regimes are subject to frequent and sometimes sudden change. Sanctions may be imposed at any time by any country, international organisation or governing body and generally take immediate effect. To manage sanctions exposure associated with the Group's clients, employees, business partners and the jurisdictions in which they are located, the Group conducts sanctions screening against the identified sanctions regimes, using a risk-based approach, before entering relationships or facilitating a transaction with clients, employees, suppliers, associates, and business partners to ensure that it does not establish a relationship or facilitate a transaction for, on behalf of, or in favour of a sanctioned individual, entity or country.

Existing business relationships, employees and business partners are screened on an ongoing basis against amendments or changes to these sanctions regimes. This is to identify any business relationship, employee or business partner who may become sanctioned after a contractual relationship has been established.

If the Group becomes aware of a potential sanctions violation, the matter will be promptly investigated and escalated to relevant senior management and Group Compliance, with full cooperation provided for any related government or regulatory investigation.

Where a business relationship or business partner becomes subject to an applicable sanctions regime, the Group will assess the matter on a risk-based, case-by-case basis, taking into account the relevant sanctions requirements, contractual provisions, local legal and regulatory obligations, and the enforceability of any decision to suspend or terminate the relationship.

Contractual clauses
The Group entrenches appropriate compulsory sanctions and general risk clauses in all contractual arrangements that allow for the unilateral termination of the contract by any entity within the Group if the client, employee or business partner becomes subject to an applicable sanctions regime.

New or high-risk jurisdictions
The Group exercises caution and carefully considers the risks involved in doing business in any new jurisdiction. The Group undertakes a risk-based assessment before entering any relationships (clients, employees or business partners) in new jurisdictions. Enhanced due diligence is triggered if there are findings in the preliminary assessment.

The Group conducts sanctions screening and risk-based due diligence investigations to vet potential clients, employees and business partners in high-risk jurisdictions, including their related parties, based on information provided by the business and available in open sources. The Group continuously monitors the status of these jurisdictions. The Group's risk assessment is updated accordingly to ensure compliance with all applicable laws and regulations.

4.3 ANTI-MONEY LAUNDERING, COUNTER-TERRORIST FINANCING AND COUNTER-PROLIFERATION FINANCING (AML, CTF AND CPF) RISK MANAGEMENT AND COMPLIANCE PROGRAMME (RMCP)

INTRODUCTION

Discovery Limited's (AML, CTF and CPF) RMCP ('programme') sets out the risk-based principles, requirements, controls, procedures, systems and standards of management of financial crime risks, including money laundering, terrorist financing and proliferation financing (ML, TF and PF) and sanctions breaches, that all employees must adhere to, to ensure that all operations are conducted in a manner that satisfies the regulatory framework. The objective of this programme is to ensure regulatory compliance and to establish an internal framework that minimises the risk of sanctions breaches and abuse of the Group's products and services for money laundering, terrorist financing and proliferation financing purposes.

LEGISLATIVE AND REGULATORY REQUIREMENTS

Discovery must comply with the relevant AML, CTF and CPF laws and may, based on its risk tolerance, adopt more exacting standards. This programme complies with international standards and the relevant jurisdiction-specific regulatory frameworks.

All employees must be familiar with the relevant policies that set out the control and governance framework including, among other things, the duties and obligations of employees relating to the prevention of financial crime and ABC practices.

MEASURES TOWARDS ML, TF AND PF AND SANCTIONS COMPLIANCE

Client due diligence (CDD)
In parallel to the establishment and verification of a client's identity, Discovery must apply a risk-based approach towards the collection, registration and ongoing monitoring of information in relation to the nature and purpose of the business relationship. Discovery will apply proportionate levels of identification, verification and risk-rating activities depending on the ML, TF and PF risks identified for each individual transaction. Discovery will implement appropriate client acceptance instructions to set clear guidance on which natural persons and legal entities are

considered as the strategic client base, with references to ML, TF and PF and sanctions risk in line with the risk assessment and risk rating methodology.

Discovery undertakes significant effort to determine the ownership and control structure of legal entities, where this is a regulatory requirement. In instances where client due diligence measures include reliance or outsourcing of controls or processes, agreements will be entered into which must comply with the applicable legislative requirement, any regulatory guidance issued in respect thereof, and Discovery's Outsourcing Policy and Procedures, including periodic reviews.

Politically exposed persons, adverse media and sanctions
To identify natural persons classified as domestic politically exposed persons, foreign politically exposed persons ('PEPs') or prominent influential persons ('PIPs'), as well as persons associated with adverse media and sanctioned persons or entities, the Group conducts screening in real time during both manual and automated onboarding processes, and on an ongoing basis after that.

Transaction monitoring and reporting
Discovery applies a risk-based approach to transaction monitoring, using both automated and manual processes to assess whether a client's activities, including the use of products or services, premium payments, claims activity and general behaviour, are consistent with the purpose and intended nature of the business relationship. Where activity appears unusual or inconsistent with the client's known profile, Discovery investigates the matter further and, where required, takes appropriate reporting or escalation action. Discovery keeps electronic records of all transactions and due diligence measures carried out in accordance with the programme.

Freeze orders
In the event of a true match against a sanctions list (jurisdiction dependent)[1], Discovery is committed to freezing the property and exiting the business relationship as legally permitted, and in line with guidance received from regulatory and enforcement bodies as promptly and as efficiently as possible. Employees are required to understand and comply with their obligations under applicable Freezing of Funds Notices, including the prohibition on dealing with, or making funds or other economic resources available to, designated persons or entities. This obligation applies across relevant business activities and must be escalated where any potential exposure to a designated person or entity is identified.

4.4 GROUP FINANCIAL CRIME RISK MANAGEMENT POLICY

Discovery's Group Financial Crime Risk Management Policy sets out the Group's overarching approach and principles for managing financial crime risk across Discovery Limited and its subsidiaries. The policy recognises financial crime as a risk to the Group, the financial services sector and broader society, and covers a broad range of financial crime risks, including bribery and corruption, fraud, misappropriation, money laundering, terrorist financing, proliferation financing, market abuse, privacy and cybersecurity-related misconduct, and other relevant offences under applicable legislation.

The policy provides for a consistent governance and risk management approach to the prevention, detection, investigation, reporting and remediation of financial crime. It is supported by clear governance arrangements, defined accountability, risk-based oversight, appropriate controls, independent review and escalation processes across the Group. It further reinforces the importance of risk assessments, appropriate controls, training and

[1] South Africa adheres to the sanctions measures adopted by the United Nations Security Council (UNSC); The UK adheres to the sanctions measures adopted by the UK His Majesty's Treasury (HMT); and The US adheres to the sanctions measures adopted by the Office of Foreign Assets Control (OFAC).

awareness, escalation of incidents, independent assurance and fair, transparent investigation processes where suspected financial crime arises.

5. VITALITY FINANCIAL CRIME POLICY MINIMUM STANDARDS

5.1 VITALITY UK FINANCIAL CRIME POLICY MINIMUM STANDARDS

Vitality UK has procedures and controls in place that are designed to deter and detect financial crime. These procedures and controls are monitored and formally assessed regularly (at least yearly). A yearly financial crime risk assessment process is in place across all operations to evaluate the internal and external risks to the business.

Procedures and controls are in place for the pre-employment vetting and recruitment of employees and contractors; customer identification and monitoring; due diligence assessments on third parties before entering any business relationship and subsequent monitoring of interactions; and monitoring of all payments and investigating deviations from established patterns. Client databases are regularly screened against various international sanctions lists.

Regular training is provided for all employees on the legal and regulatory requirements relating to money laundering; in particular, employees are trained to recognise suspicious transactions. All suspicious transactions are reported to the Group's Money Laundering Reporting Officer (MLRO), who will review and determine whether the matter should be referred to the National Crime Agency (NCA).

5.2 VITALITY UNITED STATES MARKET SEGMENT (VITALITY US) – FINANCIAL CRIME MINIMUM STANDARDS

For Vitality US, procedures and controls are in place to deter and detect financial crime, informed by applicable legislative requirements and Group minimum standards. Risk-based due diligence assessments for new partners and territories are undertaken by Discovery's Group Compliance function. These assessments cover both entity-level and country-level risks. Where required, assessment findings and outcomes are escalated through established governance processes and structures.

GLOSSARY

1. **Money laundering**
   The concealment of the origins of illegally obtained money, typically by means of complex financial transactions.

2. **Proliferation financing**
   Proliferation financing is defined by the Financial Action Task Force (FATF) as the provision of funds or financial services used for the manufacture, acquisition, possession, development, export, trans-shipment, brokering, transport, transfer, stockpiling or use of nuclear, chemical or biological weapons and their means of delivery and related materials (including both technologies and dual-use goods used for non-legitimate purposes). This is in contravention of national laws or, where applicable, international obligations.

3. **Terrorist financing**
   Terrorist financing refers to the funds generated by legal or illegal means to sustain terrorist groups and allow them to continue their operations financially. Terrorist financing includes the movement of these funds between conduits and terrorist groups.

DOCUMENT CONTROL

DETAILS

Document owner | Group Compliance Control Function

Document level | Group-wide

Level of approval | Discovery Limited Risk and Compliance Committee, Discovery Group Executive Committee.

Frequency of review | Every 2 years or out of cycle due to an operational or regulatory trigger event.

DOCUMENT APPROVALS

This document forms part of the Discovery ML/TF/PF, anti-bribery and corruption and sanctions risk and control framework and has been approved by the Group Risk and Compliance Committee and Executive Committee as applicable.