Group Speak Out Policy

Why is this policy necessary?

The purpose of this policy is to set the framework by which the Group can reinforce one of the Group's core values in the Group Code of Business Conduct: Integrity.

Key Principles

The Group is committed to fostering a culture of openness, honesty and accountability and requires the highest possible standards of professional and ethical conduct of itself and from all employees. Consequently, it is fundamental that any genuine concerns of suspected misconduct within the business are aired.

Speak Out is the Confidential Reporting system applicable across the Group and has been implemented to receive Qualifying Concerns about ethics, compliance or Group Code of Business Conduct. The Speak Out reporting programme is accessible to all employees, contractors, vendors, agents, clients in a language of their choice, and disclosure could be made through a range of communication methods. Further information is available on the Speak Out website.

Speak Out is run by NAVEX Global, a third-party supplier that specializes in ethics and compliance programs. The set-up ensures maximum confidentiality, as reports are stored on a database outside the Prudential Group environment.

Policy detail

Under this policy:

- Businesses are required to fully comply with all relevant local regulatory and statutory requirements related to Whistleblowing.

- Businesses are required to pass full details of all Priority 1 or potential Priority 1 concerns to the Group Chief Security Officer within 1 working day of the matter coming to their attention, and if the Concern relates to the Group Chief Security Officer the matter will be referred directly to the Group Legal Director, who will be responsible for overseeing the investigation.

- Reported concerns must be recorded in the Speak Out case management tool, Navex, by the conclusion of the following working day, and classified under one of the following categories: anti-bribery/ corruption; anti-money laundering laws and terrorism financing; compliance breaches; concealment; criminal offence; damage to the environment; discrimination; harassment or unfair treatment; falsification of contracts/reports /records; financial irregularities; fraud and embezzlement; health and safety; misconduct; retaliation; significant deficiencies or material weaknesses in the Group's system of internal controls; supplier or customer financial impropriety; and trading or insider information.

- Business are required to promote the existence of the Group Speak Out website and Toll-Free Confidential Reporting, to provide annual training and awareness on how to raise a concern through Speak Out in a manner and language appropriate to the LBU. Businesses must ensure that all workers are made aware that the Group has 'zero tolerance' to retaliation against

reporters of any Concerns raised through Speak Out. Training material must also be made available to contractors, vendors and agents.

- Businesses must ensure that nothing in their arrangements (including any employment contract or settlement agreement or any other related or ancillary documents) prevents or discourages employees or agents from raising Concerns directly to the local regulator, or any other body empowered to receive Speak Out reports in the relevant jurisdiction. Regulated businesses must comply with the specific requirements of their regulating body in respect of their ability to disclose concerns directly to those bodies.

- Access to the information, records and technology of the Speak Out system is strictly limited to specified, trained and suitably experienced personnel.

- Each Concern must be treated confidentially and the anonymity of the person raising the Concern is maintained when legally permissible.

- Reporters raising any Concern must not be discharged, threatened, suspended, reprimanded, harassed, disciplined, have payment of salary and/or benefit withheld or suspended, demoted, transferred or otherwise be subject to any disciplinary or retaliatory action related to the terms and conditions of employment.

- Businesses must establish, implement and maintain a framework for management reporting to the Group Chief Security Officer, including the reporting of new Concerns and updates on current cases and post-investigation remediation plans, and shall facilitate assurance activities by Group Security. The Group Chief Security Officer shall provide status reports on the effectiveness of the Speak Out reporting system and controls to the Group Audit Committee.