Whistle Blowing Policy[1]

Foreword

At RUSI, we seek always to conduct our business honestly and with integrity, and to comply with all legal requirements that govern our activities. However, we also acknowledge that, despite these efforts, all businesses face the risk of their activities going wrong from time to time, or of unknowingly harbouring malpractice.

'Whistleblowing' is the term used when a worker passes on information concerning wrongdoing. The wrongdoing will typically (although not necessarily) be something they have witnessed at work. To be covered by existing whistleblowing law, a worker who makes a disclosure must reasonably believe that they are acting in the company's or the public's interest, and that the disclosure tends to show past, present or likely future wrongdoing.

Application

This policy applies to all individuals working at all levels of the organisation, including trustees, employees, consultants, interns and other voluntary workers, casual and agency staff as well as all sub-contractors, suppliers and partners, together known as "RUSI Staff".

To reiterate, it applies to all consultants and subcontractors when it comes to their engagements with RUSI. This means that consultants and subcontractors will be required to report any incidents in relation to the conducts described below if they impact in any way their engagement with RUSI or relate to a project/contract in which RUSI is involved.

Conducts Which Require Reporting

Compliance with applicable laws and regulations implies not only preventing malpractice but reporting it to RUSIs senior management who may in turn report it to competent authorities when applicable. RUSI Staff are therefore under an obligation to report suspicions in relation to the following conduct:

- Fraud, bribery, and corruption
- Violations to safeguarding or modern slavery regulations
- Harassment, bullying and discrimination
- Money laundering, terrorism financing and attempts from terrorist organisations and individuals to abuse RUSI.

[1] This policy does not form part of any employee's contract of employment, and it may be amended at any time.

- Breaches to RUSI's cybersecurity policies and incidents which may endanger RUSI's operations, or the information stored by RUSI as well as persistent negligence that may threaten RUSI's cybersecurity policies.
- Serious incidents which could potentially or have effectively put RUSI Staff in any form of danger and which may threaten their physical, psychological and/or emotional wellbeing.

All concerns or suspicions in relation to the conduct described above should be reported as described herein. RUSI will take all reports seriously and ensure that the circumstances which have triggered a report are investigated thoroughly. Whistle-blowers will be protected from any form of retaliation and all information provided by them will be subjected to the strictest confidentiality. RUSI Staff who victimise or retaliate against those who have raised concerns under this policy will be subject to disciplinary action.

If an investigation under this policy concludes that a disclosure has been made maliciously, vexatiously or with a view to personal gain, the whistle-blower will be subject to disciplinary action or, in the case of a consultant or subcontractor, the termination of the relevant contract.

Covering up someone else's wrongdoing is a disciplinary offence or a potential breach of contract. RUSI staff should never agree to remain silent about a wrongdoing, even if told to do so by a person in authority such as a manager.

Reporting Channels

- Allegations of harassment, bullying and/or discrimination should be reported to the line manager as established in the Grievance policy and procedure. Internal matters between RUSI staff will be investigated and resolved by HR. If, for whatever reason it is not possible to report an incident to the line manager, the Director of HR may be contacted directly.
- Suspicions related to fraud, bribery, corruption, money laundering, terrorism financing, violations to safeguarding and/or modern slavery policies, as well as serious incidents should be reported to the Risk and Compliance Manager, as well as suspicions related to other criminal activities not listed herein.
- Any issues identified by subcontractors and consultants should be reported through the email feedback@rusi.org.
- Breaches to RUSI's cybersecurity policies and procedures or attempted cyberattacks should be reported to the Chief Operating Officer (COO).
- Any reports which involve the Director of HR or the Risk and Compliance Manager may be reported directly to the COO to avoid conflicts of interest.

All reports related to fraud, bribery, corruption, money laundering and serious incidents will be investigated by the Risk and Compliance Manager to determine whether there are additional reports that require filing with UK authorities. The following are some of the mandatory reports which may need to be filed depending on the circumstances:

- A Suspicious Activity Report (SAR) should be filed to the United Kingdom's Financial Intelligence Unit (UKFIU) via the National Crime Agency's SAR Portal[2] when there is a suspicion of money laundering or terrorism financing
- All serious incidents should be reported to the Charity Commission[3]
- If potential involvement from a terrorist organisation or individual is detected in relation to a specific transaction or project, it must immediately be reported to the Police[4]. If the situation is considered an emergency, 999 must be contacted without delay.
- Concerns in relation to money laundering and tax evasion should be reported to the Charity Commission as well as the HM Revenue and Customs (HMRC).
- Situations of fraud should be reported to Action Fraud.[5]

Any incidents related to the conduct described in this policy and which impact or relate to any contract with the Foreign Commonwealth and Development Office (FCDO) must be reported to said entity through one of these channels:

- Email: reportingconcerns@FCDO.gov.uk
- Phone: +44 (0)1355 843747

When filing a report, it is not necessary for the whistle-blower to have proof that such an act is being, has been or is likely to be committed. A reasonable belief is sufficient, even if that belief later turns out to be wrong. The whistle-blower has no responsibility for investigating the matter and should not attempt to do so. It is management's responsibility to ensure an appropriate investigation takes place.

If a member of RUSI staff has a complaint relating to their personal circumstances in the workplace, they should use the normal grievance procedure set out in the Staff Handbook.

Content of Reports, Investigation and Record Keeping

Whenever the need to file a report arises, the whistle-blower must include as much information and describe in as much detail as possible the events which have generated the concern. At the very least a report will require the following for an investigation to be possible:

- Name of the individuals or project the events relate to
- The specific events which generate a suspicion of unethical, criminal or dangerous behaviour
- The date on which the events took place
- The names of any individuals who might either be in danger or have been harmed or may be in any way affected by an event or conduct.

All information provided will be considered confidential and the identity of the whistle-blower will only be disclosed if requested under warrant by a competent authority or if so authorised by the whistle-blower themselves.

[2] https://www.ukciu.gov.uk/(im4his45uydcgeeik5epkbjo)/saronline.aspx
[3] https://register-of-charities.charitycommission.gov.uk/reporting-or-updating-a-serious-incident
[4] https://www.met.police.uk/tua/tell-us-about/ath/possible-terrorist-activity/
[5] https://www.actionfraud.police.uk/reporting-fraud-and-cyber-crime

A case number will be assigned to each report and a case file will be opened by the Risk and Compliance Manager in which all information related to the report and subsequent investigation will be recorded. Reasonable efforts will be made to determine if suspected unethical, criminal or harmful behaviours have indeed occurred. If after an investigation is conducted it is determined that there is sufficient evidence to indicate other authorities need to be informed, all required reports will be filed, with the prior approval of the COO, and copies of said reports will be saved. The Chair of the Audit and Risk Committee will also be informed of the situation. Finally, Trustees will receive a briefing at their next meeting, on any incidents which required reporting to external authorities and the circumstances that led to the report.

On the other hand, if no indication of wrongdoing is found, the investigation will be concluded. Results of investigations may rarely be shared with whistle-blowers as authorities often require that decisions to file reports remain confidential.

If in addition, an investigation triggered by a report requires disciplinary action to be taken in regard to one of RUSI's staff, all appropriate internal policies and regulations will be observed.

When an investigation concludes that one of RUSI's suppliers or subcontractors is involved in any of the conducts subjected to reporting as per this policy, all contractual relationships will be terminated without there being grounds for compensation.

Version control

Author	First drafted	Approval date and approving body	Latest update
Andrea Plazas	11/2022	15/12/2022 – Approved by Senior Management	15/12/2022