Whistleblowing 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 person passes on information concerning specified types of wrongdoing. These are also known as qualified disclosures. The wrongdoing will typically (although not necessarily) be something they have witnessed at work.

This policy is intended to cover incidents of all levels of seriousness. Most incidents of wrongdoing can and should be dealt with through the regular reporting channels defined below. For exceptional situations where more serious wrongdoing is suspected the exceptional reporting channels, also below, can be used. The final option for where the most serious of wrongdoing is suspected a disclosure under the Public Interest Disclosure Act 1998 can be made.

Those making qualifying disclosures are protected against dismissal or detriment by The Public Interest Disclosure Act 1998. A "qualifying disclosure" means a disclosure of information that you genuinely and reasonably believes is in the public interest and shows that the Organisation has committed a "relevant failure".

These acts can be in the past, present or likely to happen in the future. The Employment Rights Act 1996 provides protection for workers who 'blow the whistle' where they reasonably believe that some form of illegality, injustice or breach of health and safety has occurred or is likely to occur. The disclosure has to be "in the public interest". We encourage you to use the procedure to raise any such concerns.

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, collectively known as "RUSI Representatives". All RUSI Representatives are 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.

Should the concern not meet the requirement to be a qualifying disclosure or be appropriate for any of the other reporting channels named below, you should raise it under RUSI's grievance policy, held in the HR

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

The Royal United Services Institute
61 Whitehall, London
SW1A 2ET
United Kingdom

+44 (0)207 747 2600
enquiries@rusi.org
rusi.org
@RUSI_org

area of SharePoint. If a concern is raised under the whistleblowing policy when it is not appropriate to do so the receiving manager will confirm that the matter will be addressed under the grievance policy.

Regular Reporting Channels

The regular reporting channels for suspected wrongdoing are set out below:

- A failure to comply with a legal obligation should be reported to the CFO.
- A miscarriage of justice should be reported to the Director of HR.
- Endangering the health and safety of an individual should be reported in line with the Health and Safety Policy held in the HR section of SharePoint.
- Environmental damage should be reported to the CFO.
- Suspicions related to fraud, bribery, corruption, money laundering and terrorism financing, violations should be reported to the CFO.
- Breaches of RUSI's Safeguarding and Modern Slavery policies should be reported as outlined in the respective policies.
- Any issues identified by subcontractors and consultants should be reported through compliance@rusi.org.
- Breaches to RUSI's cybersecurity policies and procedures should be reported to the CFO.
- Allegations of harassment, bullying and/or discrimination are not generally classed qualifying disclosures and should be reported to the line manager as established in the Grievance policy.
- Potential or actual conflicts of interest should be reported directly to the HR Director as stated in the Conflict of Interest Policy.
- Any situation that could call RUSI's academic integrity into question should be reported to the Director of Research.
- Any reports which involve the Director of HR may be reported directly to the CFO to avoid conflicts of interest.
- Serious incidents and suspicions related criminal activities not otherwise listed should be reported to the Chief Financial Officer (CFO).
- Any other problems that are not mentioned elsewhere in this policy can be reported directly to the Director of HR.

Exceptional Reporting Channels

Anonymous reports to RUSI may be made through the use of the Microsoft Form in the Risk and Compliance area of SharePoint.

In truly exceptional and rare circumstances where there is suspicion of major wrongdoing by RUSI management, e.g. concealing any information relating to the above mentioned relevant failures, a report may be made directly to the Chair of the Audit and Risk Committee. Currently the Chair of the Audit and Risk Committee is Laurence Geller, his contact details are held on the CRM.

The Royal United Services Institute
61 Whitehall, London
SW1A 2ET
United Kingdom

+44 (0)207 747 2600
enquiries@rusi.org
rusi.org
@RUSI_org

All reports related to fraud, bribery, corruption, money laundering and serious incidents will be investigated by the CFO or other appropriate authority to determine whether there are additional reports that require filing with UK authorities. This will occur after an internal report has been filed through internal channels. The following are some of the mandatory reports which may need to be filed after an internal investigation 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].
- Concerns in relation to money laundering and tax evasion should be reported to the Charity Commission as well as 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

Reports

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.

When reporting a problem, the whistle-blower must include as much information and the events in as much detail as possible. To begin an effective investigation the following details must be included:

- 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.

[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

The Royal United Services Institute
61 Whitehall, London
SW1A 2ET
United Kingdom

+44 (0)207 747 2600
enquiries@rusi.org
rusi.org
@RUSI_org

The more information provided the more effective 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 authorised by the whistle-blower themselves.

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.

Investigations

When a report is made a case number will be assigned and a case file will be opened by the member of staff that receives the report. Said case file will contain all information related to the report and a record of the subsequent investigation. 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 CFO, 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.

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 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.

If an investigation concludes that one of RUSI's suppliers or subcontractors is involved in any of the conduct subject 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
Peter Clarke	DEC-25	SMT DEC-25	MAR-26

The Royal United Services Institute
61 Whitehall, London
SW1A 2ET
United Kingdom

+44 (0)207 747 2600
enquiries@rusi.org
rusi.org
@RUSI_org