Anti-terrorism policy

1. Scope of the policy

This policy sets out IDS' position in relation to anti-terrorism laws and regulation that the Institute and its Trustees are subject to. It provides an overview of activities and expectations in regard to ensuring that the Institute operates within the laws of the UK regulations of the Charity Commission, as well as the laws of other jurisdictions that become relevant through any aspect of the Institute's work. The policy also provides colleagues with advice on how to navigate broad and sometimes complex anti-terrorism laws where they present a greater risk than usual within research projects and other activity undertaken by the Institute.

Any breaches of anti-terrorism laws may lead to serious consequences for IDS, including custodial sentences for staff and Trustees in addition to fines, loss of charity status and consequential reputational damage. It is therefore important that all colleagues take time to read and understand the requirements of this policy and to seek advice where they are unsure as to when and how it applies to their work.

This policy shall supplement any other forthcoming guidance and papers under the umbrella theme of conducting research in high risk settings and those under the auspices of authoritarian governments.

2. Law and regulations

- The primary laws of relevance regarding the activity of the Institute are: the UK Terrorism Act 2000; the Terrorist Freezing Act 2010; and the UK Counter-Terrorism and Border Security Act 2019.

A description and the key considerations of each Act is as follows:

- **UK Terrorism Act 2000**

  Offences that fall under this Act are broad and can include activities that take place within and outside of the UK. The main offences that an individual or organisation can purposely or inadvertently commit include meeting with (within the UK) or supporting members of a proscribed organisation, providing money or property for the purpose of terrorism or legitimising proscribed organisations through the expression of an opinion or belief that may encourage others to support or legitimise the proscribed organisation/person.

- **UK Terrorist Freezing Act 2010**

  Offences can include a UK national or incorporated group making funds or financial services available (directly or indirectly) to a proscribed organisation or designated person anywhere in the world. A designated person can be an

organisation or an individual if they are listed on the HM Treasury or the EU consolidated list of frozen assets. There are no financial thresholds that apply to financial or other material support under this act, so any payment made directly or indirectly to a proscribed person, or anyone operating on their behalf may be a breach of this law.

- **UK Counter-Terrorism and Border Security Act 2019**

  The most recent UK counter-terrorism law, although controversial as to its possible ramifications for humanitarian and research organisations, creates a new offence of entering or remaining in an area outside of the UK that has been designated as a no entry zone by the government. Amendments to the Act passed in Parliament in 2019 exempts those providing humanitarian aid through NGOs and it is generally accepted that the exemption applies to academics conducting research even if this is not explicitly stated within the Act itself. Designation will likely apply to areas of Syria and Iraq in time, but other areas of the world may be designated at the discretion of the Home Office if the area meets the designation criteria under the Act. Travel to any area designated under the Act therefore carries an extra element of risk to colleagues so additional scrutiny of the purpose and necessity of the travel should be considered.

  In addition, the Act expands upon elements of the Terrorism Act 2010 to cover viewing or making available certain material online which could be useful to a terrorist - it extends the offence of inviting support for a proscribed organisation through the expression of supportive opinions. Even if there is no intention to invite support for a proscribed organisation, the application of law may determine that a reasonable person should have foreseen this as a consequence.

Due to its charity status, IDS must also comply with the regulations and the statutory powers of the Charity Commission which can be exercised in parallel to UK counter-terrorism laws. Charity Commission guidance is generally cautious and broad-brush in nature with an emphasis on ensuring that charities should not be benefitting terrorist organisations, financially or otherwise. A key principle of the Charity Commission guidance is that Trustees have a duty to ensure that their charity 'must not engage in conduct or activities which would lead to a reasonable member of the public to conclude that the charity or its Trustees are associated with a proscribed organisation or terrorism generally'.

This places a broader responsibility on the Institute and its Trustees since the inference is that no crime must be alleged or committed for the Charity Commission to take concern over any incidents that may arise. In short, the Charity Commission guidance for Trustees includes the following:

- Comply with the law, including counter-terrorism legislation.

- Act in the charity's best interest, avoid exposing it to undue risk and make sure assets are used only to support its charitable purposes.
- Take reasonable steps to ensure that a charity's premises, assets, staff, volunteers and other resources cannot be used for activities that may, *or appear to*, support or condone terrorism or terrorist activities.
- Ensure that effective procedures are in place and properly implemented to prevent terrorist organisations taking advantage of the charity's status, reputation, facilities or assets.
- Take immediate steps to dissociate the charity from any activity that may give, or appear to give, support to terrorism or terrorist activity.
- Take all reasonable steps to ensure that the charity's activities are open and transparent so that these cannot be misinterpreted.
- Exercise proper control over the charity's financial affairs and safeguard its assets.

Any incidents that concern counter-terrorism laws should be reported to the Charity Commission. See section six for more information on reporting.

Compliance with the laws under the jurisdiction of non UK-based funders will also need to be considered where they apply. The counter-terrorism laws of the USA for example are even more expansive and extraterritorial in their scope than those of the UK, with the assertion of jurisdiction over both US and non-US nationals. Counter-terrorism requirements of a relevant country are always included within funding agreements and these should be reviewed and understood prior to the start of any work.

3. Responsibilities

- The Board of Trustees have accountability for the Institute's compliance with counter-terrorism laws, charity law and the Institute's proper discharge of duty in relation to the Institute's charitable objectives and its allocation of resources. It is responsible for ensuring that risks taken by the Institute are done so reasonably, diligently and do not exceed a level that may lead to legal, regulatory, or reputational harm.
- Managers shall ensure that their staff are aware of this policy and the related policies as listed in section seven and should support their staff in its application where needed.
- All staff are responsible for reading this policy and considering where and how it applies to their role and the projects they work on.
- Project leaders should ensure that terrorism risks are adequately considered within project risk registers and that adequate mitigation measures are in place during the life of their projects.

4. Considerations for research projects

Anti-terrorism risk, that is the risk of non-compliance with counter-terrorism law, is not present to the same degree across the Institute's research projects and may be more acute in some projects over others. The key drivers for risk will typically relate to the geographical location of the work, the stakeholders involved and the choices around partnerships, but the following indicators will mean a heightened anti-terrorism risk:

- Elements of work will be conducted in areas under the authority of a proscribed entity or where proscribed organisations and its members are known to be heavily present.
- Elements of work will be conducted in areas designated under the Counter-Terrorism and Border Security Act 2019.
- It may be necessary to engage members of a proscribed organisation for research purposes, including the need to gain access to certain areas or project beneficiaries.
- The in-country presence of proscribed organisations and complex networks may mean that contact with members may be made unintentionally.
- The work requires involvement of in-country partners that are unknown to IDS or do not have a demonstrable track record of regular international funding streams from other trusted donors and partners.
- The outputs from the project may include findings regarding proscribed organisations that a member of the public may view as an attempt to legitimise their interests.

In addition to the measures outlined under section five below, Annex 1 of this policy outlines further projects risks and actions.

5. Risk mitigation

Risk assessments

As with all complex research projects, thorough risk assessments are required during the design/proposal phase and on an ongoing basis. Projects should create and maintain a risk register for the project and include a section on counter-terrorism where there is a heightened risk according to the indicators listed under section four.

Where the indicators are present, it is vital that the reporting steps outlined under section six are followed.

It is IDS policy to provide the right levels of oversight, guidance, and support toward delivering on the objectives of the project insofar as possible when balanced against the Institute's legal and regulatory responsibilities. Depending on the degree of risk, a special oversight committee - including nominees from the Board of Trustees, Strategic Leadership Group and other relevant colleagues

- may be established in order to provide assurance that risks to the Institute and individuals do not exceed an acceptable level. The project will also be included within the strategic risk register until the anti-terrorism risks have been managed.

Due diligence

The IDS due diligence policy should apply to all organisational partners prior to them undertaking work or establishing a contractual agreement. If the due diligence policy is followed, this will help to mitigate anti-terrorism risk as the due diligence will cover and provide assurance regarding several related areas including:

- Verification that the partner is legally established within their countries of operation.
- Evidence of their internal policy and control framework regarding all aspects in the use of forward funds provided by IDS.
- Declarations to confirm that the partner is not aware of any terrorism incidents within their organisation or extended networks.
- Evidence of the partner's capacity and experience including track record in receiving and managing funds from reputable donors and other partner organisations.

Screening lists

IDS operates an automated screening process. Whenever a new individual or organisational record is created, the information will be included within the next screening cycle. Screening works with an algorithm that cross checks the Customer Relationship Management (CRM) contact and organisational records against terrorism and financial watch lists. These lists currently include:

- Home Office list of proscribed groups and organisations.
- HM Treasury consolidated list of financial sanctions targets in the UK.
- EU consolidated list of persons, groups, and entities subject to financial sanctions.

A weekly sanction list report of any potential matches is generated and sent to the Contracts and Compliance Manager who will look further into any potential matches and will escalate in the unlikely event that a positive match is suspected. To date, no positive matches have been flagged within the reports.

The limitation to the screening process is that the details of the organisations and individuals must be in the CRM system to be part of the automated process. Therefore, it is important for projects teams to a) ensure that partner information is gathered and added to the CRM as soon as is feasible to do so and b) if work involves groupings of unknown individuals that would not normally be entered into CRM, lists containing information on the individuals/organisations involved should

be passed to the contracts and compliance team who can run additional ad-hoc screening checks.

Country sanctions

International banking regulations - commonly known as 'Know Your Customer' (KYC) -require increased scrutiny of relationships and financial disbursements to partners in certain countries. This additional scrutiny provides a layer of anti-terrorism protection because the Institute's banking provider will also conduct their own screening checks prior to authorising payments. However, banks will also expect the Institute to be proactive with regards to supporting KYC requirements. In addition to the application of due diligence under the IDS due diligence policy, the finance team have in place an early alert system for new sub-contract records that concern any 'restricted' or 'narrowly restricted' countries according to banking regulations. The countries currently restricted or narrowly restricted are listed in Annex 2 and are on the IDS contracts and compliance intranet page: https://instdevelopmentstudies.sharepoint.com/sites/intranet/SitePages/Contracts.aspx

If a new proposal or project record in the CRM is created that includes a country from the restricted or narrowly-restricted lists, these will be added to a weekly report that flags the existence of these to the Contracts and Compliance Manager and the senior financial accountant, responsible for maintaining the banking relationship. This provides the relevant teams with an early read of the pipeline of potential and new projects that may present a greater risk to the Institute.

If a new sub-contract partner record is created within the CRM and where the partner is based in a restricted or narrowly-restricted country, a notification is automatically sent to the Contracts and Compliance Manager and senior financial accountant who will:

- Request details from the project team on the intended sub-contract.
- Check to ensure that due diligence for the partner has been conducted to the right standard and is recorded on the Institute's systems.
- Conduct any necessary additional screening or due diligence checks.
- Inform the bank of the intended sub-contract, provide them with the details we have and ask the bank to check that payments can be made to the partner within the banking regulations.

Where any issues are identified, these will be communicated to the project teams along with any options in rectifying issues that may be available.

Whilst the outlined steps above will take place once a sub-contract partner record is created, the sooner relevant colleagues are informed of a project team's need to sub-contract partners in the restricted and narrowly-restricted lists, the sooner we are able to confirm that we can make payments within the regulations.

6. Reporting, approvals and incidents

To adequately manage anti-terrorism risk, it is important that the right reporting channels are used both internally and externally. This section outlines the reporting steps that all colleagues should be aware of and use when concerned about anti-terrorism risk.

1. Where a project or areas of the Institute's activity involves a heightened anti-terrorism risk or if an unanticipated incident occurs or if a complaint is received, this should be escalated in the first instance to the Director of Finance and Operations in his/her capacity as Chair of the Risk-Management Subcommittee.

2. The Director of Finance and Operations may seek more information and where satisfied that the risk to the Institute is not greater than would be expected within any project, may approve the project to proceed whilst providing any further stipulations. If the risk to IDS is deemed greater than would be usually expected, the Director of Finance and Operations will escalate the issue to the attention of the Director, the Strategic Leadership Group and the Risk Management Sub-Committee.

3. The Strategic Leadership Group may seek more information and escalate the matter to the Board of Trustees at their discretion.

Where an oversight committee is established following the engagement of the Strategic Leadership Group and the Board of Trustees, other communication requirements will be established including to the project's funder and relevant project partners or the public. The oversight committee will advise on mitigation plans, frequency of updates and will be responsible for providing go/no-go decisions with the following stipulations considered:

a. The work is in-keeping with Institute's strategy and clearly furthers the Institute's charitable aims and objectives.
b. There is evidence of sufficient risk assessments and mitigations in place.
c. The work shall not place IDS, its staff or Trustees at risk of legal or regulatory consequences.
d. All staff and partners involved in the work must be able to do so safely and in line with the IDS travel and security policy.

It may not always be possible to anticipate all anti-terrorism risks in advance and situations can occur in real time. If there is an incident or concern that wasn't previously anticipated and reported as per this policy, these should be raised as soon as possible to the Director of Finance and Operations and to the Director of Research. The Directors will seek to establish the facts of the incident to determine if any activity has occurred that places the Institute at undue risk or if any further reporting channels need to be used.

In addition to the steps above, it is important to note that where colleagues have concerns that the Institute is not exercising its duties adequately or legally in relation

to anti-terrorism risks, the IDS whistleblowing policy is available for anyone to report concerns in confidence within IDS or to appropriate external bodies where necessary.

Please note that other standard approvals, such as approvals for travel under the travel and security policy are still required in parallel to those required under this policy where they are relevant.

7. Related policies and key contacts

Managing anti-terrorism risk is a multi-faceted endeavour and therefore this policy is to be read and understood along with the following related policies that all contribute toward the Institute's approach in managing such risks:

- Financial procedures manual: sets out how the Institute practices sound financial management and operates on principles of segregation of duty and financial oversight.
- Anti-bribery, corruption and money laundering: covers matters such a facilitation payments and other matters that have a close association with anti-terrorism risk.
- Due Diligence: documents the standards for conducting due diligence on partner institutes, including verification of their legal standing, reputation, and ability to manage project funds with diligence and to the equivalent standards of the Institute.
- Risk management: provides guidance and requirements for the Institute's sound management of project and institutional risk more broadly but with principles that apply to management of anti-terrorism risk.
- Travel and security: provides the protocols around preparing for and conducting travel, including in higher risk and fragile settings, and protocols around incidents such as terrorism attacks.

If any colleagues require advice or support in relation to the application of this policy, the following people can help:

- Director of Research
- Director of Finance and Operations
- Contracts and Compliance Manager
- Senior Financial Accountant

Issue Number	Date	Changes Made	Owner	Approved By
1	May 2020	First Issue	Muz Roberts	Strategic Leadership Group

Annex 1. Project risk and mitigation guidance for projects in designated or higher risk locations in the context of anti-terrorism lists.

Risk	Mitigation
Project work located within designated country/area under UK counter-terror law	- Treat as high-risk travel under the travel and security policy, complete secondary risk assessments and ensure approval sought in advance - Review legal implications for designation status - Subject to travel approvals, carry appropriate documentation, permits, letters of support from the institute - Collaborate with trusted in-country partners
Meeting with proscribed organisations and their members/affiliates outside of the UK (such as to facilitate access to field work sites or project beneficiaries)	- Avoid wherever possible - If not possible to avoid: a. ensure meetings are held in private b. ensure meeting agenda is decided in advance and recorded, and minutes and meeting records are accurately recorded and retained c. under no circumstances should payments or exchange of materials/goods take place to secure site access etc. d. If a situation has developed suddenly without the opportunity to gain prior approval, ensure that the situation is reported to IDS as soon as possible after the event.
Proscribed organisation member participation in project workshops	- Avoid. This may provide such members with a platform to encourage support or legitimacy
Payments to individuals and organisations	- Only make payments to individuals where their identity and circumstances can be verified. - Where identification can be obtained, pass details to contracts and compliance team for additional screening checks

	- Ensure all partner organisations have had due diligence checks completed and recorded under the due diligence policy - Engage trusted in-country partners to support verification of identities and to make local contacts
Public statements and research findings	- Ensure public statements about the project include clear articulation of the benefits of the project and the ways in which it furthers IDS' charitable objectives - Findings regarding proscribed organisations should be objective and evidenced based to avoid members of the public to consider an association between IDS and the organisation or an attempt to legitimise their cause - Engage with IDS communications team prior to release of statements or publications for an assessment of the language and messaging in the context of counter-terrorism law.

Annex 2. Restricted and narrowly-restricted countries

Restricted countries	Narrowly-restricted countries
Cuba	Afghanistan
Iran	Belarus
North Korea	Burundi
Sudan	Central African Republic
Crimea	Congo, The Democratic Republic of the
Syria	Egypt
	Eritrea
	Guinea
	Guinea-Bissau
	Iraq
	Lebanon
	Libyan Arab Jamahiriya
	Mali
	Myanmar
	Russian Federation
	Somalia
	South Sudan
	Tunisia
	Ukraine
	Venezuela
	Yemen
	Zimbabwe