TRUSTED RESEARCH

Implementation – collaboration checklist

Evaluating research proposals

National Protective Security Authority

National Cyber Security Centre

This checklist is a resource which may be used by researchers and research offices to determine the level of risk incurred by a collaboration.

At the outset of a collaboration, the researcher and research office may wish to discuss who will take responsibility for the varying elements of this checklist to avoid duplication while ensuring compliance. Depending on your institutional processes, the division of the checklist questions between the researcher and the research office may vary.

In line with your institutional policies and processes, you should exercise your own judgement on which of the below questions are most applicable to informal and formal collaborations.

Upon completion of the checklist, you may wish to contextualise the answers to the below questions with your institution's risk appetite to determine whether to move forward with the collaboration, and if so, then identify which mitigations you need to put in place.

This checklist does not intend to be an exhaustive list but provides a range of considerations which should help researchers and research offices to take an informed view on the risks posed by a particular collaboration.

This checklist may be used as a starting point for:

- identifying risks which need to be mitigated
- identifying legal obligations which must be met
- considering whether the collaboration needs to be escalated within your institution for approval
- considering the wider policies which govern your institution and whether the potential partnership aligns with your institution's values
- considering your existing partnerships, including with funding bodies, and any contractual obligations which must be upheld

Research considerations

- ○ Is your research sensitive?
- ○ Does your research have any dual-use (both military and civilian) applications?
- ○ Are there any ethical or moral concerns for the potential applications of your research? **Considering this question may help you to establish whether your research could be used to undermine UK national security.**
- ○ Could your research be misused or have any unintended applications which could be exploited by third parties to undermine UK national security if they obtained your research?
- ○ Do you need to protect sensitive data or personally identifiable information (e.g. genetic or medical information, population datasets, personal details, commercial test data)?
- ○ Will your prospective partner be granted access to your institution's IT network? What wider visibility of your institution's research and data could this give them?

Partner considerations

- ○ Is your prospective partner based in or from a country which has differing democratic and/or ethical standards from the UK? **Considering this question may help you to establish whether your prospective research partner, or the government of their home country, may seek to act against the interests of the UK's national security.**
- ○ How does the country in which your prospective partner is from or based approach academic freedom and open science? Does their approach to these ideas provide you with any cause for concern?
- ○ Is the prospective partner subject to any organisational structures or relationships that could compromise their independence or integrity? Are there any sources of unwanted control or influence?
- ○ Is your prospective partner based in or from a country where its government, military, police force or security services are hostile to the UK?
- ○ Is your prospective partner linked to foreign governments, militaries, police forces or security services? If so, are these entities viewed as hostile to the UK?
- ○ Is your prospective partner assessed to be at a high-risk of diverting assets to a foreign military, police force or security service?
- ○ Is your prospective partner, or any institutions they are associated with, on the US entity list?[1]

1 https://www.ecfr.gov/current/title-15/subtitle-B/chapter-VII/subchapter-C/part-744/appendix-Supplement%20No.%204%20to%20Part%20744

Legal considerations

- ○ Are there any legal or regulatory considerations or constraints on undertaking your research with this partner (e.g. DPA, GDPR, ATAS, visas)?
- ○ Is any of the research likely to be subject to UK or other countries' export licence controls?
- ○ Is your prospective partner, or any institutions they are associated with, on the UK government end-user list?
- ○ Does your research fall within any of the 17 sensitive areas of the UK economy as defined by the National Security and Investment Act?
- ○ Is the prospective partner, or an organisation linked to them, subject to a sanction by the UK, UN or other sanctioning body?

Institutional considerations

- ○ Are there any university policy constraints on undertaking your research with this partner?
- ○ Does the decision to undertake this collaboration need to be escalated within your institution?
- ○ Are there complex considerations which require input from external bodies (e.g. RCAT, ECJU etc.)?

Reputational considerations

- ○ Have you established why this prospective partner wants to work with you?
- ○ Has your partner funded or partnered with an entity whose values or intentions do not align with your institution's own values? **Considering this question may help you to establish whether a prospective partner may be more likely to act, or be compelled to act, in a way that is contrary to the UK's national security.**
- ○ Has your partner been involved in civil or criminal proceedings?
- ○ Have you identified any information that does not match with what your partner told you, suggesting a lack of transparency on their part?
- ○ Is the prospective partner seeking to deviate from internationally recognised norms and technical standards?

Contractual considerations

- ○ Would proceeding with this partner raise potential conflicts of interest with existing research partners or funders?
- ○ Would proceeding with this partner breach any existing contractual agreements you have with other partners or funders?
- ○ Do you have a responsibility to provide existing partners or funders with visibility of new partnerships?
- ○ Would it be necessary to put in place additional protections between the research undertaken for prospective proposal and any existing research seeking to answer similar research questions?

Intellectual Property (IP) considerations

- Do you need to protect any existing IP? If so, is the IP considered high-value or sensitive?
- Has the prospective partner been accused of IP infringement and/or theft?
- Are there any indications that the prospective partner, their parent organisation or their government are amassing IP in your research area?
  Considering this question may help you to establish whether your prospective partner appears to be attempting to uplift a specific capability for an overseas nation. If this capability has military applications, this could be damaging to the UK's national security.
- If the prospective partner is international, are they operating under local laws which may put your IP at risk?
- Does your prospective partner intend to take full or majority ownership of the IP? If so, what are the possible consequences of this action?
- Who is the ultimate beneficial owner of any IP resulting from the collaboration?
- Do you have plans in place for protecting the IP resulting from this collaboration? In which jurisdiction(s) will those protections be upheld?
- Is your research likely to have a future commercial or patentable outcome which you or your organisation would want to benefit from?

Strategic considerations

- Would the collaboration erode UK capabilities, particularly in areas of UK strength or nascent growth, and/or national security?
- Would the collaboration create, or contribute to, financial dependence on the prospective partner or financial leverage either over you or the institution?
- Does your research have the ability to uplift potentially malign capabilities in foreign states?

Disclaimer

This resource has been prepared by NPSA and NCSC and is intended to aid academic institutions to help them understand and mitigate security risks arising from research, in combination with additional resources and the application of institutions' own judgement. This document is provided on an information basis only, and while NPSA and NCSC have used all reasonable care in producing it, NPSA and NCSC provides no warranty as to its accuracy or completeness.

It is important to emphasise that no security measures are proof against all threats. You remain entirely responsible for the security of your own sites and/or business, and compliance with any applicable law and regulations. You must use your own judgement as to whether and how to implement our recommendations, seeking your own legal/professional advice as required.

To the fullest extent permitted by law, NPSA and NCSC accept no liability whatsoever for any expense, liability, loss, damage, claim or proceedings incurred or arising as a result of any error or omission in the document or arising from any person acting or refraining from acting, relying upon or otherwise using the guidance. This exclusion applies to all losses and damages whether arising in contract, tort, by statute or otherwise including where it is a result of negligence. NPSA and NCSC separately and expressly exclude any liability for any special, indirect and/or consequential losses, including any loss of or damage to business, market share, reputation, profits or goodwill and/or costs of dealing with regulators and fines from regulators.

Institutions and individuals have a responsibility to ensure that they comply with all relevant legal obligations, as well as any other obligations to which they are beholden. This guidance included in this document should not be considered exhaustive. This guidance raises issues for consideration but does not dictate or purport to dictate what conclusions institutions should reach.

OGL

© Crown Copyright 2024

This publication is licensed under the terms of the Open Government Licence v3.0 except where otherwise stated. To view this licence, visit nationalarchives.gov.uk/doc/open-government-licence/version/3

You may use or reuse this content without prior permission but must adhere to and accept the terms of the Open Government Licence for public sector information.

You must acknowledge NPSA as the source of the content and include a link to the Open Government Licence wherever possible. Authorisation to reproduce a third party's copyright material must be obtained from the copyright holders concerned.