UK Research and Innovation

UK Research and Innovation

Trusted Research and Innovation Principles

August 2021

Introduction

UKRI has a long-standing commitment to effective international collaboration in research and innovation; UKRI is equally committed to ensuring that this takes place with integrity and within strong ethical frameworks. To ensure that research and innovation in the UK continues to thrive, international collaboration must be safeguarded. To create an environment that allows international partnerships and open research to flourish, all parts of the sector need to engage in positive risk awareness, adopt key mitigation and risk protocols that minimise threats and empower researchers, innovators and organisations to make informed decisions.

Purpose

The following UKRI Trusted Research and Innovation Principles set out UKRI’s expectations of organisations funded by UKRI in relation to due diligence for international collaboration. This applies to new grants and existing grants. Organisations funded by UKRI should adopt these principles and be able to evidence the controls and measures that have been put in place that are consistent with these principles.

1. Assessment of Partner Suitability

An appropriate due diligence assessment should be undertaken of potential financial and non-financial collaborative partner organisations and/or individuals in relation to the areas outlined below. Examples of factors that could be taken into consideration when identifying risk are the nature of the project activity and the envisaged outputs; the potential for unethical or dual-use of project information and/or outputs; the potential for fraud, bribery and corruption; and the collaborating partners.

Where a risk to the project findings and the potential usages is identified, reasonable and proportionate mitigations should be implemented in line with the UKRI funded organisation’s risk appetite prior to the collaboration being agreed. If a change to a partner organisation’s circumstances becomes known, the UKRI funded organisation should consider undertaking further due diligence in line with its risk appetite. A record of this assessment should be held by the UKRI funded organisation in line with their own retention polices.

Legal Framework and Affiliations

An understanding is required of the legal framework and constitution of the partner organisation and/or the country in which it operates, who it is owned by and whether it has any formal affiliations with other entities such as other businesses, government departments or the military. If any affiliations pose a potential risk to the integrity of the handling of project information or project outputs, then mitigations should be put in place in line with the organisation’s risk appetite. Organisations should also be aware of any obligations applicable to them under the National Security and Investment Act.

Values

It is important to understand the democratic and ethical values of the country that the partner is based in and where these might differ from our own. There are various resources that could support organisations in recognising potential risks associated to the project and when mitigations may be required, depending on the nature of the project and the partners involved; for more details please see ‘Further Information’.

Conflicts of Interest

Ensuring an individual-level awareness of people interacting with your organisation is essential to assessing potential security related risks. Appropriate due diligence can be undertaken in line with your organisation’s risk appetite to identify existing or potential conflicts of interest posed by individuals who will have physical and/or virtual access to your organisation via employment, study, collaboration, visits or access to data. Risk indicators that could be considered include whether a person has any military affiliations, other sources of income, other employment, and upheld allegations of breaches of research integrity or ethical standards.

2. Managing Information and Knowledge Sharing

Transparency and openness are integral to the success of research and innovation, without this the benefits of such activity cannot be fully realised. However, this requirement must be balanced with the need to safeguard information and knowledge sharing. It is therefore essential that organisations have robust information security management measures in place to ensure that access to sensitive data and information is appropriately managed. Organisations should be mindful of the information and knowledge they are sharing, even in assisting researchers/funders in interpreting data and using technologies/facilities.

Cyber Security

A robust cyber-security culture achieved through the development of cyber controls introduced as part of a security awareness and training program that includes well-publicised guidance for staff and students, is essential for reducing the risk of cyber-attacks.

Separation of Data

Sensitive data must be securely stored and, where a shared platform is used for information exchange, data should be logically separated into different locations so that it is only accessible by authorised individuals.

Access to Data

Access to sensitive data should only be given to individuals with a clear requirement for access, for the duration that such access is required. The basis for the handling and usage of the data should be clearly specified, understood and agreed by all parties prior to information being shared. It is important to be aware of any local legislation that may apply to overseas partners that might permit authorities to access sensitive information without consent from all parties.

Project Activity and Outputs

All project activity and the handling of project outputs must be compliant with applicable export control legislation and any other legal requirements. In addition, due consideration should be given toward the nature of the project activity and envisaged outputs, regarding the potential for dual-use and unethical application. Further guidance is available from the Centre for the Protection of National Infrastructure and the Export Control Joint Unit.

3. Commercial Application

Collaboration agreements should be in place to ensure that sensitive data and any intellectual assets including intellectual property rights derived from the project are appropriately managed, particularly where there is potential for future commercial outcomes to be realised which could benefit society and the economy including that of the UK.

Intellectual Assets and Intellectual Property Rights

The intellectual assets including any intellectual property arising from the project should be managed in a professional and business-like manner. This might include deciding when it is most appropriate to seek protection for the intellectual property arising from the project and subsequently how to exploit, assign, license or disseminate it to maximise its impact. This must not conflict with UKRI’s mission “to convene, catalyse and invest in close collaboration with others to build a thriving, inclusive research and innovation system that connects discovery to prosperity and public good.”

Publishing Project Outputs

Notwithstanding UKRI’s mission, prior to any collaboration all partners should formally agree when commercially relevant and/or sensitive data and/or findings derived from the project can be made publicly available. Where necessary, it may be appropriate to seek protection for the knowledge asset including any intellectual property prior to its publication or for a high-level version to be published instead. When a decision is made to publish research findings, the outputs should comply with UKRI’s open access and open data policies and guidance.

Export Controls

UK export controls are designed to restrict the export and communication of sensitive technology, knowledge or strategic goods and apply equally to the academic community as to any other exporter. All organisations funded by UKRI should ensure they understand export controls that may apply to their project and activities, from the export of materials to presentations at conferences. There are tools to check any restrictions or requirements regarding export control licenses and it should be noted that failure to comply with these controls may result in a criminal offence being committed.

Further Information

Additional guidance and supporting information can be found from the following resources:

- Centre for the Protection of National Infrastructure (CPNI) “Trusted Research” guidance for the research and innovation sector
- Universities UK (UUK) Managing risks in Internationalisation: Security related issues
- Universities UK (UUK) Oversight of Security – Sensitive Research Material in UK Universities - Guidance
- Academic Technology Approval Scheme (ATAS)
- Export Controls Applying to Academic Research
- Trade Restrictions on exports: detailed information
- Export Control Unit -.GOV.UK
- National Security and Investment Act