Royal Academy of Engineering
Policy on National Security-Related Risks

1. Introduction

This policy primarily addresses the risk that technology or knowledge developed as part of the work that the Academy supports could be misused by a foreign state to build capacity to target UK interests in a hostile fashion, or to control or repress their population. It also looks to support wider measures to ensure the security and integrity of the UK research and innovation sector, and its international partnerships.

2. Scope

This policy applies to all Academy activities, but at present primarily focuses on our research and innovation grant giving activities and work with international partners, as those are where these risks are most significant at present. It applies to all staff, Fellows, others assessing grant applications, Academy grant holders and recipient organisations.

3. Policy Statement

1. The Royal Academy of Engineering is the UK's National Academy for engineering and technology, and we are proud of the contribution that engineering and technology make to the security of the United Kingdom and its allies. In all our activities we seek to minimise the risk that technology developed as part of work that we support could be misused by a foreign state (or hostile actors) to build a capacity to target UK interests in a hostile fashion, or to control or repress populations.
2. We strongly support the UK government's focus on science and technology as a source of strategic advantage. Hence, we also support measures to make it more difficult for potentially hostile states to gain access to sensitive UK research information, whilst seeking to make sure that those measures are not so burdensome as to harm the advantage that they are looking to protect. We will work with partners across the UK research system to support the security and integrity of the UK's research system.
3. The Academy is committed to playing a progressive leadership role in all aspects of diversity and inclusion within engineering and technology. We therefore strongly reject any behaviours that use national security concerns as an excuse for prejudice or hostility towards UK researchers of a particular ethnicity or nationality, or similar non-inclusive behaviour.
4. We are concerned that the Academy, given our connections to many of the UK's leading engineering centres, may be a target for organisations seeking to gain unauthorised access to intellectual property. We are likewise concerned that the Academy's beneficiaries, both in the UK and around the world may similarly be targeted by organisations seeking to gain unauthorised access to intellectual property. We therefore make this policy public to highlight how the Academy and its beneficiaries should respond to this developing set of risks.
5. We seek to support both the vitality and the integrity of the system of international research and innovation collaboration, which is vital to the continued success of the UK's research and innovation sector, and the realisation of many benefits around the world. We highlight the guidance provided by the National Protective Security Authority (NPSA) (formerly Centre for the Protection of National Infrastructure (CPNI)) on Trusted Research https://www.npsa.gov.uk/trusted-research as central to that goal.
6. We highlight that the UK government has issued guidance on how export control legislation applies to academic research: https://www.gov.uk/guidance/export-controls-applying-to-academic-research. This highlights that whilst there are exemptions for knowledge already in the public domain and for basic research, they do apply to applied research collaborations and taking research overseas. Failure to apply for the required licence can potentially carry severe criminal sanctions. Many of the Academy's activities support applied research, making knowledge of these controls particularly important for our community.
7. We are committed to working globally, supporting excellent engineers around the world to promote social benefit, and convening international partners to develop solutions and systems that will help address the most pressing global challenges. We acknowledge that in doing so, we and our awardees will work with engineers from nations that have a wide range of

relationships with the UK, including some where there are concerns of potential adversarial relationships.

8. This policy shall be updated from time to time reflecting new regulatory positions and any improved understanding of the risks to be managed. An up-to-date version can be found here: https://raeng.org.uk/programmes-and-prizes/programmes/uk-grants-and-prizes/support-for-research/programme-policy-documents
9. Summary of Requirements

For All

- To seek to minimise risks that technology developed as part of work that the Academy supports could be misused by a foreign state to build a capacity to target UK interests in a hostile fashion, or to control or repress their population.
- To treat national security related risks with the requisite degree of care and diligence.
- To remain strongly committed to diversity and inclusion in all activities, remembering that national security concerns must never be used as an excuse for prejudice or hostility towards UK researchers of a particular ethnicity or nationality.
- If standard communication routes are not judged appropriate, to report concerns about national security-related risks according to the Academy's Whistle Blowing Policy and Procedure.

For Academy grant holders

- To be aware of and comply with this policy.
- To be vigilant against any risk that their work may be adopted by a foreign state's military or similar hostile organisation against UK interests, or be misused by a state to control or repress populations.
- To report to the Academy any concerns about National Security that arise in their work. In particular, to report through their usual Academy contact point if they take on any new role associated with a foreign government and if they plan any new partnership with a defence firm or military organisation outside the UK.
- To take note of the guidance provided by the National Protective Security Authority (NPSA) (formerly Centre for the Protection of National Infrastructure (CPNI) on Trusted Research (https://www.npsa.gov.uk/trusted-research).
- If involved in an innovative start up company, to note the guidance from NCSC and NPSA on Secure Innovation: https://www.npsa.gov.uk/secure-innovation and to be aware of the legal requirements of the National Security and Investments Bill 2020.
- To be aware of the potential application of Export Controls to applied engineering and technology work and to abide by those laws, seeking guidance and support from their hosting organisation to do so.
- To attend training events around National Security risks organised by the Academy.
- To abide by any specific risk mitigation plans put in place on grants.
- To highlight to the Academy if they believe their hosting institution is not providing them with suitable specialist support for managing risks around international collaborations.

For Research and innovation institutions applying for or hosting Academy grants

- To provide specialist support for their research staff around risks in international collaboration, export controls and related issues. This must be done in a way that ensures that researchers are not expected to undertake due diligence on their own projects. Rather, such checks should be the responsibility of experts in international collaboration risks not directly engaged in the same project. The costs of such specialist support should be considered an essential part of a well-founded applied technology research activity.
- To work in line with evolving sector guidance such as Universities UK's report on "Managing Risks in Internationalisation: Security Related Issues in Higher Education", by Professor Sir Peter Gregson FREng:

https://www.universitiesuk.ac.uk/policy-and-analysis/reports/Documents/2020/managing-risks-in-

internationalisation.pdf

- To link with the government's Research Collaboration Advice Team within the Department for Science, Innovation and Technology (DSIT), which promotes government advice on security-related topics, such as export controls, cyber security and protection of intellectual property, and other specialist groups for sharing knowledge across the sector.
- To be aware that failure to suitably support research staff or to manage risks in National Security issues (in any activity, not only those directly funded by the Academy) may lead to an organisation being declared ineligible for Academy funding or being asked to give formal assurances to retain eligibility for Academy funding.
- To report to the Academy any concerns about National Security that arise in conjunction with any Academy funded work. In particular, to highlight if the awardee takes on any new role associated with a foreign government.

For Fellows and others making decisions on grant applications

- To support security mindedness in all aspects of the Academy's activities.
- To be mindful of potential national security concerns surrounding any application to the Academy for support or nomination to become a Fellow, and to alert the panel chair and supporting staff about any such risks.
- To be aware that failure to declare a national security related concern related to Academy activities can be considered grounds for an investigation into misconduct under the Fellows Code of Conduct.

For Academy Staff

- To be aware of and comply with this policy.
- To be aware of and comply with the Procedure Document for this policy (Annex A in the internal version) and in particular how it applies to grant making and international partnerships work.
- To notify a member of the Academy's National Security Risks Group of any national security related concerns of which they become aware.
- To ensure their attendance and that of their direct reports at national security risk training, as requested by Academy National Security Risks Group.
- To be aware that failure to declare a national security related concern can be a disciplinary offence.
- To include any national security related risks within risk registers at organisation, team, scheme or other levels as appropriate.

4. Roles and Responsibilities

For all groups, to comply with the requirements in section 9 of part 3 above.
The National Security Risks Group chaired by the Executive Director, Programmes, has responsibility for updating this policy and the associated National Security Risks Procedure Document. As appropriate, it may consult Audit and Risk Committee or relevant Academy Operating Committees for comment and advice on those procedures. This group includes: the Executive Director of Programmes; Associate Director, Research Programmes and Awards; Head of Grants Processes and Operations; Head of Risk and Compliance; Associate Director, International; Associate Director of Engineering Policy; and Head of Innovation, Analysis and Public Affairs. This group will review any concerns on national security risks and decide on the Academy's response, possibly after consultation with specialist representatives of government, expert Fellows, and Chairs of responsible steering groups and committees.

5. Procedures

The Academy has developed and will continue to evolve appropriate procedures to uphold the Policy commitments under the oversight of the National Security Risks Group chaired by the Executive Director, Programmes. These procedures can be found in the National Security Risks Procedure

Document.

6. Training

The Academy will ensure that appropriate training is delivered to impacted staff, Fellows, award holders and relevant external contributors, including new starters.

7. Related policies and other references

See National Security Risks Procedure Document

Version history

VERSION	AUTHOR	LEAD DIRECTOR	APPROVED BY	DESCRIPTION OF CHANGE	DATE OF APPROVAL
1	Andrew Clark	Andrew Clark	Trustee Board	New	10/07/23