JUNE 2022

Managing risks in international research and innovation

An overview of higher education sector guidance

Universities UK

CPNI
Centre for the Protection of National Infrastructure

UKRI
UK Research and Innovation

Contents

Introduction

This briefing summarises key themes from guidance for the higher education sector on managing security-related issues in international research and innovation. It also provides some case studies on how the guidelines have been used by universities to support their risk management processes.

Internationalisation has shaped the agenda and strategies of universities not just in the UK, but globally. It has brought significant economic and social benefits to the UK, and intellectual opportunities for scholarship, while transforming universities into global institutions. Collaboration with international partners continues to be vital to the continued success of the UK's research and innovation sector.

However, there are risks associated with internationalisation, which are increasingly dynamic and growing in complexity. Because of this, institutions have continued to review and adapt their risk management processes.

Numerous guidelines have been developed to support universities, helping them to protect themselves, their staff and students, and to manage risks associated with internationalisation.

About this briefing

This briefing is a high-level summary of key principles and guidelines produced by Universities UK (UUK), the Centre for the Protection of National Infrastructure (CPNI) and UK Research and Innovation (UKRI). It will outline the main principles set out in these three documents and provide examples of how they have been implemented by universities.

It complements other pieces of guidance on security-related issues, many of which are outlined in Further resources. It aims to help UK universities be confident and able to pursue sustainable, secure international partnerships.

This briefing is not intended to replace the original principles and guidelines produced by UUK, UKRI and CPNI. It should be read in conjunction with and alongside the original documents. **We strongly advise that you read these in full.**

Existing guidance

The three specific pieces of guidance referenced here are:

CPNI, Trusted research guidance for academia

This 2019 guidance outlines the potential risks to UK research and innovation. It's designed to help researchers, UK universities and industry partners to have confidence in international collaboration and make informed decisions around those potential risks, and to explain how to protect research and staff from potential theft, misuse or exploitation.

UUK, Managing risks in internationalisation: security-related issues

This 2020 guidance provides detailed guidance for universities on considerations and measures they should take to guard against hostile interference and promote academic freedom.

It covers four broad areas:

1. protecting your reputation and values
2. protecting your people
3. protecting your campuses
4. protecting your partnerships

UKRI, Trusted research and innovation principles

UKRI published these principles in 2021 to support recipients of UKRI funding when considering their approaches to ensuring trusted research and innovation. They provide guidance on how to assess partner suitability, how to manage information and knowledge sharing, and legal and security implications of the commercial application of research collaboration and outputs.

Overarching aims, threats, risks, and mitigations

The aim	The threat	The risk to universities	The mitigations
• To enable universities and research organisations to protect their organisation, people and research from security threats. • To ensure that students, staff, and faculties have their rights and sensitive information. protected. • To uphold and strengthen the reputation and integrity of the UK higher education and research sectors.	The most serious national security threats addressed by the guidance are state threats to research. Other threats include cyberattacks, fraudulent business proposals, terrorism, and the abduction or harm of students and staff overseas.	Failure to mitigate against these threats will also result in more immediate risk to the organisations. This includes reputational risk, financial loss, litigation (export control, NSI), and the violation of the rights of students and staff.	• identifying sensitive research • due diligence on partners • good governance with risk management coordinated and endorsed from the top • staff training and awareness • appropriate information management and sharing, • proportionate physical and personnel security • legal compliance

Threats and intended outcomes

It's important to identify and mitigate potential threats to your organisation, staff and research.

State threats are the most prevalent national security threats, but organisations face a range of other risks from state and non-state actors, who may:

- seek personal financial or social gain through actively hostile and illegal actions, such as cyber attacks, or through fraudulent or legally ambiguous business proposals and practices
- seek opportunities to increase their own economic, technological and military advantage over other countries
- seek to deploy their technological and military advantages against their own people or cultivate PR opportunities to gloss over systemic human rights violations, legal and financial irregularities and adverse publicity

The nature of threats, and the threat actors themselves, are not static. State and non-state actors may target and seek to exploit academic institutions and collaborations – for example, to transfer or steal information and intellectual property. Cyber attacks are just one method. Physical access to research sites and personnel offered by academic collaboration are also effective in obtaining and transferring or compromising research and expertise.

Research and expertise can be accessed and transferred through academic institutions, state-linked entities, and private companies and individuals. Failure to protect research, data and staff can result in financial and reputational damage to your organisation and staff and damage to the integrity of your research. It may even compromise national security.

By taking these issues seriously, universities can help to:

- protect their people and campuses
- protect their reputation and values
- protect their research and partnerships
- protect trust in UK higher education

To achieve this, universities must:

- understand their education and research partners
- understand their obligations
- communicate effectively with staff on threats, policies and their role in mitigation
- take proportionate actions to mitigate these risks

Collectively, by addressing these risks and implementing these mitigative actions, institutions not only protect themselves but help guarantee the collective security and reputation of the sector and of the UK as a trusted partner.

More information about these threats and intended outcomes of the guidelines are outlined in the Mitigation checklist.

Implementing the guidelines

To manage risks effectively, universities must have sound governance, with clear leadership and robust processes in place to identify, evaluate and mitigate risk.

This is not unique to security-related risks, and universities will already have such systems and processes in place. However, the novel and evolving nature of security-related risks does mean that these require special attention.

Universities will ensure there is senior-level visibility and accountability of the security of international collaborations and partnerships. They should also adopt a risk-management approach, and create a culture of security-mindedness. Universities should also promote a culture of awareness and communicate and reinforce individual and collective responsibilities.

The response to security-related challenges should be periodically reviewed so that the university's policies and processes evolve as necessary to cope with current threats.

Suggested first steps

1. Appoint a member of your senior leadership team to take responsibility of security-related matters.

2. Review the three major pieces of guidance outlined in this briefing, and any other relevant guidance.

3. Assemble a team of stakeholders across your institution that have expertise in the recommended areas.

    - This may include, but not be limited to, the following teams:
        - research
        - international
        - recruitment
        - management and support
        - recruitment and student support

- It may also include professional services, such as the following teams:
  - IT
  - estates
  - HR
  - finance
  - operations
  - teaching
  - legal

4. Review existing related processes and identify a list of recommended actions, with proposed leads and timescales, that you can turn into a project plan and present to your executive and/or board.

5. Set out an action plan with clearly defined senior responsibility owners and reporting. Examples of actions universities have taken include, but are not limited to:

   - unifying due diligence management across departments, eg research, finance, and philanthropy
   - expanding risk registers and sharing them across teams in a given institution
   - upgrading due diligence processes and checks
   - updating, revising or creating policies on institutional values, academic freedom and freedom of speech
   - improved policy and training programmes, staff training on security related matters, and creating new working groups or reporting processes
   - conducting cyber-attack and physical penetration tests to update virtual and physical security infrastructure
   - 'stress testing' policies, such as using phishing email tests, visitor simulations, and crisis procedures against use cases

6. Ensure that security-related matters are on the radar of the governing board of your institution, and that developments are communicated appropriately. UUK guidelines recommend that the governing board of an institution receive an annual report on security risks.

7. Develop a plan to ensure that practitioners, academics, and broader academic services staff are aware of policy updates and their rationale and buy-in to the reasons for updates and changes. These plans should be regularly revisited and reviewed to reflect changing security priorities and threats.

Embedding security-mindedness across an institution

1. Ensure that you have two-way conversations with academics and wider professional staff early on. It's important that security matters are understood across the whole institution, and that they are seen as enabling rather than hindering.

2. Many universities have found that appointing internationalisation or security champions in different teams and faculties has worked well, as people tend to trust information coming from their peers. Departmental champions will understand day-to-day applicability and apprehensions better than professional services staff.

3. Ensure internal resources such as webpages are clear, up to date, and easy to access, ideally with named points of contact for further questions.

4. Develop and clearly communicate points of contact on security issues to support internal discussions.

5. Have conversations across all teams and departments. Security-mindedness is not limited to research and partnership departments – it also relates to teaching, students services, students themselves, and other stakeholder groups who might not initially think that security issues concern them.

6. Tailor your message to your audience, making sure that it is practical, supported by supplementary material, and of appropriate complexity. Both messaging that is too complex and too simple can be unhelpful.

7. Develop clear messaging from senior leadership on how security issues are a priority.

8. Acknowledge that concerns are legitimate. Brushing concerns aside is counterproductive. Focusing on how security-mindedness enables excellent research and teaching, and that security measures exist to enable staff, is more productive than dismissing concerns.

9. Seek opportunities to engage in sector-wide conversations around security issues, to share reliable information and good practice.

10. Consider where training might be helpful.

Training

The Royal Society has produced a training package in collaboration with CPNI which helps raise awareness of trusted research and national security considerations.

Royal Society grant recipients will receive this training in 2022–23. The package will then be updated in line with feedback from Royal Society participants with a view to making it available to a wider sector audience. The insight, experience and resources provided by the Royal Society have been invaluable in shaping this package and ensuring that it's relevant to researchers.

The Higher Education Export Control Association also runs training programmes aimed at upskilling university staff in risks related to export control legislation, sanctions, and licensing. Their website also hosts resources and guidance on this topic.

Case studies

How have universities been thinking about threats, risks and mitigations?

Case study 1: University of Strathclyde

At Strathclyde, our security agenda is wide, running across many aspects of university organisation and academic culture.

When the first guidance documents were developed and launched by CPNI and UUK, our first step was to organise a workshop within the university with representatives of many different professional service and academic groups, and including vice deans and the chair of the university ethics committee.

This enabled us to develop a good understanding of where different existing responsibilities lay and how well aligned existing technical and organisational developments were with security-related issues. Most importantly, it highlighted both the opportunities and weaknesses in terms of the cultural challenge.

The understanding we gained from this initial review has informed much of our subsequent work on security-related issues. For example, it led to our strong support for, and involvement in, the sector's work on export control and the formation of the Higher Education Export Control Association (HEECA).

In terms of cultural change, we recognised a lack of understanding of the security agenda, but also two key opportunities. First, given Strathclyde's strong and long-standing industrial links, many academic colleagues were used to thinking about the responsibilities that come when working with a non-academic partner while meeting their academic goals. Second, research integrity is broadly understood as encompassing the key principles of good academic practice, and so should also encompass security. As a result, we decided to incorporate information on security-related issues through our research integrity portal.

The broad nature of the security landscape means it needs embedding in multiple areas of university work. We are investing in further underpinning capability around export control. The recent appointment of our first chief data and information officer has further boosted ongoing work on cybersecurity, as it's at the heart of their strategy development. We have also just appointed an executive level chief compliance officer, who will support the continued development of security-mindedness at Strathclyde.

Case study 2: Imperial College London

Our current approach at Imperial is to build on our well-established principles of academic rigour and integrity.

We aim to implement a culture of security-mindedness by cultivating an attentive and responsible community. Our research community and decision makers should be well-informed, enabling them to identify risk in collaborative work and the possible downsides to certain opportunities.

We're actively raising awareness of security-related issues and the legislative backdrop through an ongoing series of seminars and forums with academic departments and faculty committees. Alongside this, we have robust processes for legal compliance. In particular, we have dedicated resources for developing and managing export licensing, and triage procedures to meet the requirements of the National Security and Investment Act.

Knowledge is fundamental to all of this, and organisationally, Imperial takes a critical view of:

- **Who:** How well do we know them? What is their standing at law? Are they aligned to our values?
- **What:** What are we doing? Are there sensitivities to the activity? Is anything subject to control?
- **Where:** Where is the activity being conducted? Are any sensitive, or embargoed destinations involved? Are exports taking place?

We've established processes for due diligence. More recently, this includes additional scrutiny processes for interactions or activities deemed to be sensitive. The process allows for review of evidence by a committee, and the committee may advise conditions for continuation, suspension or even termination of the proposed activity.

This is a reiterative and ongoing process. Dedicated time and resource is important to reach and maintain the right level of capability, in particular access to sector specific tools and information to enable managed and consistent compliance.

Case study 3: University of Manchester

Over the last few years at the University of Manchester we have, like other research intensive universities, progressively strengthened our capability to address the growing number of risk areas and legal or regulatory requirements that collectively comprise the security agenda.

We have introduced new policy content, new procedures and up-to-date communications across these vital topics.

However, we also recognise that the growing complexity of the security landscape, with new legislation arriving frequently, presents additional challenges. How can we support our research community to understand when and how to engage with the multiplicity of different processes that could be applicable to their work? And how can we ensure that concerns about potential process burdens do not present a barrier to researchers who want to address global challenges in their research?

To address this, we have developed a new online research risk profiler. This tool can help researchers navigate a large range of potentially complex risk and compliance topics when planning a new project to ensure that it can proceed safely and securely. It's structured as a series of questions about a research project, which profiles potential risks and brings together relevant university advice and guidance from security-related issues resources.

The tool connects researchers with specialist professional services colleagues and teams who can support them in navigating relevant risk and compliance processes. Profiled risk areas include trusted research topics such as partner assessment, export controls, the Academic Technology Approval Scheme (ATAS), information security and IP, as well as related areas such as research ethics, travel risk and safeguarding.

Using this tool will allow researchers to better model a range of risk profiles when planning their research project and identify where projects will require additional time and support to set up. They will also be able to better understand the risks associated with their projects and the processes they may be required to complete.

Our project team worked with a number of researchers to develop the tool and, following feedback, we have ensured that guidance is provided throughout to help junior researchers and also more experienced researchers when they are planning a new project in a different research area.

We hope the tool will develop organisational awareness of security issues and promote a collective approach to addressing them across the university.

Mitigation checklist

1. Protecting reputation and values

Universities' governance structures should empower individuals, helping to promote a culture that enables staff and students to pursue international collaborations and mitigate potential risks in line with a university's risk appetite.

Universities should develop a risk-informed culture, incorporate security-related issues into relevant policies and build a culture of collective responsibility.

Universities can support this by:

- establishing security-related risk management as a key, ongoing priority
- developing board level ownership and visibility of national security risks to research and the organisation
- appointing a member of the senior leadership team as the lead on security-related issues
- knowing partners and making risk-informed decisions based on robust due diligence, eg through risk assessment of potential financial and non-financial collaborative partner organisations or individuals
- establishing key staff responsibilities
- promoting open and transparent discussion
- developing codes of conduct and policies, with mechanisms to raise concerns, and communicate these across the university and departments

Institutions must continue to promote their autonomy, freedom of speech and academic freedom.

2. Protecting research

When collaborating with both financial and non-financial research partners, it's important that universities protect intellectual property, make informed decisions and manage cyber risks.

Universities can help protect research by:

- using and understanding legal frameworks, export controls and GDPR
- protecting and sensitively storing personal and research data
- developing, implementing and reviewing cybersecurity strategies, including controlling and monitoring access to data

- considering the nature of the project or research activity

Researchers should understand which areas of their research are most sensitive, including research that is commercially sensitive, related to national security technology, or could have future dual-use or unethical applications.

3. Protecting people and campuses

Researchers are aware of the measures taken to protect themselves and an organisation's research. This includes protecting staff working overseas, and understanding the implications of working with researchers from overseas.

Universities should help researchers to stay safe when they are attending conferences abroad or working with overseas researchers, and processes and procedures should promote the safety and welfare.

Universities can support this by:

- developing internal and external communications and knowledge sharing processes
- identifying points of contact within institutions
- planning appropriate travel arrangements
- conducting appropriate due diligence and risk assessments
- developing integrated estates and visitor policies, eg frameworks, checks on visitors, strategic oversight on visitor agreements, and clear information, advice and guidance for visitors and staff on protocols

Understanding education and research partnerships

When collaborating, it's important to recognise the security implications for your university and for your research partner, and determine how suitable the collaboration is.

Universities should undertake appropriate due diligence to understand the security of supply chains and partners, and ensure that this process is ongoing and evolving.

This should help universities to:

- understand the UK's legal frameworks and those of partners and/or the countries in which they operate
- understand the democratic and ethical values of the country that a partner is based in and where these might differ from the UK
- manage any conflicts of interest and changes to circumstances
- segregate between physical and online research programmes
- protect competitors and understand their contractual expectations
- demonstrate transparent research commitments and activities
- consider steps to safeguard, and develop exit strategies for, transnational education partnership

Further resources

- UUK, Managing risks in internationalisation: security related issues
- UUK, The National Security and Investment Act: guidance for universities
- CPNI, Checklist for academics
- CPNI, Trusted research senior leaders guide
- CPNI, Countries and conferences – travel advice for academics
- CPNI, Trusted research implementation guide
- CPNI, Response to the Current Situation in Ukraine
- UKRI, Trusted Research and Innovation Principles
- UKRI, Trusted Research and Innovation Principles Q&A
- Higher Education Export Control Association
- Wilton Park, Enhancing security to support international collaboration in the Higher Education sector – exploring 'Trusted Research'

Research Collaboration Advice Team (RCAT)

The Research Collaboration Advice Team (RCAT) is a recently formed team based within the Department for Business, Energy, and Industrial Strategy (BEIS).

The RCAT provides research institutions with a first point of contact for government advice about national security risks linked to their international research portfolios. Advisers from the RCAT offer a route by which universities can access advice, as well as seek confidential consultation on sensitive and emerging security-related topics, such as research partnerships, export controls, cyber security, and the protection of intellectual property for particular international research collaborations.

RCAT advisers are distributed into regional teams based in BEIS offices throughout the UK. These advisers are building trusted one-to-one relationships with research institutions in their regions and will provide a consistent point of contact for senior research leaders.

RCAT advisers also ask questions about how a university currently manages international research risks. The responses to these questions are not being used to judge institutions or to audit them on their current practices. They will be used to build an idea of how risk is being managed across the sector, so that best and effective practices can be identified and shared. All engagement with the RCAT is on a non-mandatory basis and the RCAT has no regulatory role.

Universities UK is the collective voice of 140 universities in England, Scotland, Wales and Northern Ireland.

Our mission is to create the conditions for UK universities to be the best in the world; maximising their positive impact locally, nationally and globally.

Universities UK acts on behalf of universities, represented by their heads of institution.

Universities UK

Woburn House
20 Tavistock Square
London, WC1H 9HQ

+44 (0)20 7419 4111
info@universitiesuk.ac.uk
universitiesuk.ac.uk
@UniversitiesUK

June 2022

ISBN: 978-1-84036-491-0