CPNI
Centre for the Protection of National Infrastructure

TRUSTED RESEARCH

GUIDANCE FOR SENIOR LEADERS

National Cyber Security Centre
a part of GCHQ

Trusted Research aims to protect the integrity of the system of international research collaboration, which is vital to the continued success of the UK's research and innovation sector.

The **Trusted Research** campaign has been developed by the Centre for the Protection of National Infrastructure (CPNI) and the National Cyber Security Centre (NCSC) to raise awareness of the risks associated with research collaborations that involve organisations or research partners with links to nations whose democratic and ethical values are different from our own.

This guide accompanies the **Trusted Research** booklet and is designed for senior University leaders to have the key issues and questions at their fingertips.

Introduction

International collaboration is the cornerstone of the research and innovation sector in the UK. The International Research and Innovation Strategy (BEIS) sets out how the UK will open up the research and innovation system to international partnerships; this is crucial to the continued success of UK research.

Trusted Research provides advice on how international collaboration can be undertaken securely to maintain the world-leading reputation of UK research organisations and universities.

Good Governance

Identify a lead at senior leadership level to take responsibility for protecting your research collaborations.

Ensure that you have senior-level visibility of the security of international research collaborations and partnerships. Reputational, ethical and national security risks associated with international collaboration should be regularly discussed at senior leadership level.

Ensure that there is a clear policy which helps staff identify and highlight high-risk research activities to senior leaders. Support a **Trusted Research** approach across your institution.

Identify your most sensitive research

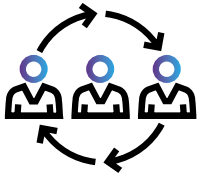
Some areas of research will be more at risk than others, so consider whether your research is commercially sensitive, has potential for patent, is related to sensitive defence or national security technology and/or could have future dual-use or unethical applications.

Consider the impact on your institution and its reputation if sensitive research or intellectual property was lost or misused by nations who have different democratic or ethical values from our own.

Identify the threats

Identify the potential threats to your most valuable research assets. Hostile state actors target universities to access personal data, research data and intellectual property. A hostile state is one whose democratic and ethical values are different from our own and whose strategic intent is hostile to the UK.

Have in place appropriate policies and processes so that staff know how to report issues or concerns. Consider sharing information with other universities and research organisations to help identify emerging threats and to learn from others.

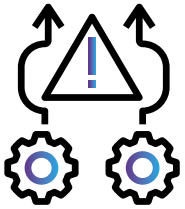


Due diligence

Ensure that your due diligence processes consider reputational, ethical and national security risks.

Consider using publicly available information to enhance your understanding of prospective research partners and their links to other research programmes, activities or states which may be of concern.

If you identify concerns about prospective partners, consider the nature of the proposed research and whether this raises reputational, ethical and national security risks.



Adopt a risk management approach

Balance risks associated with international collaboration, partnership and funding against the benefits from overseas funding and research capacity.

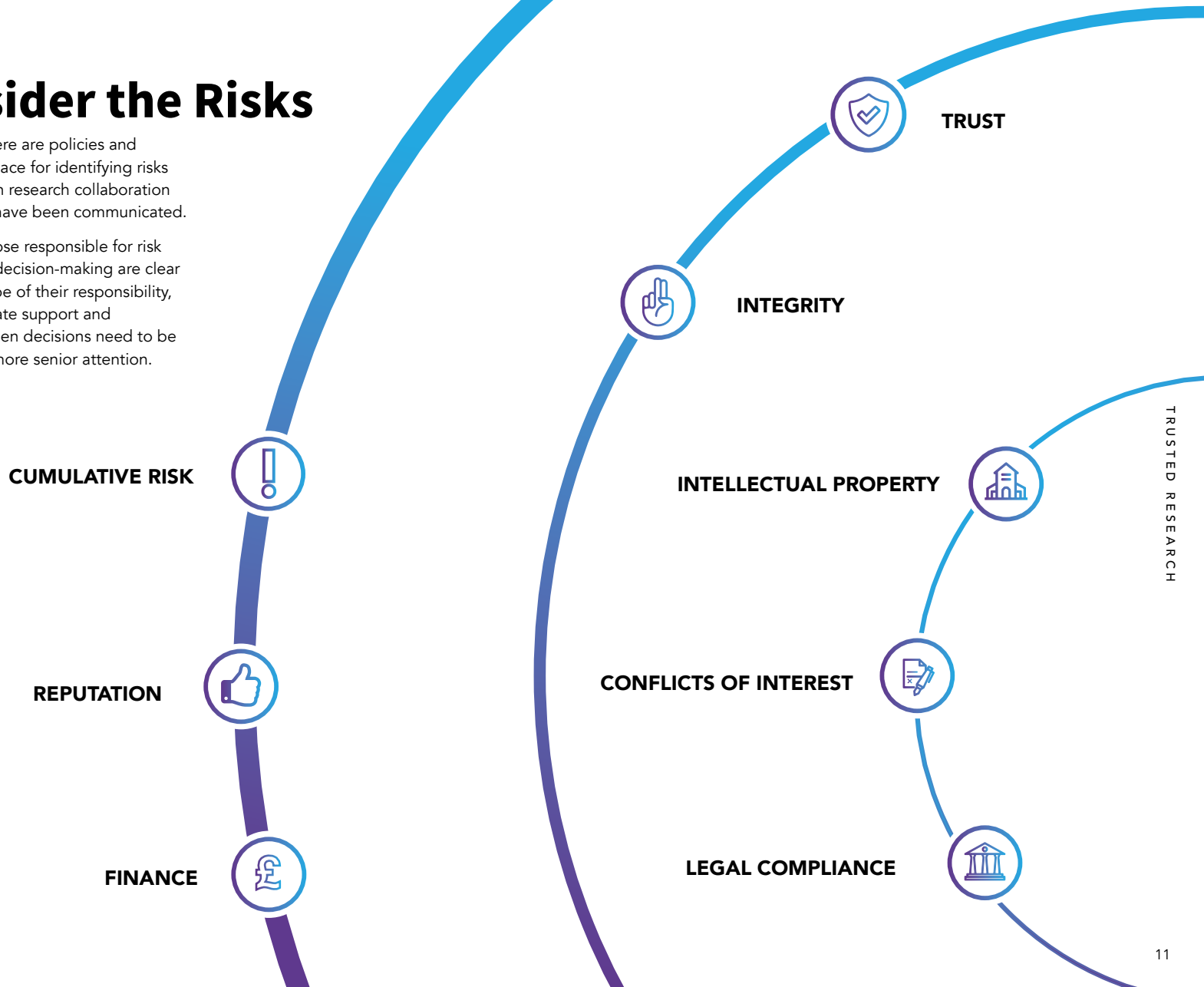
Identify what your institution values the most - the 'crown jewels' of your research portfolio – and focus your strategy on protecting it.

Choose a risk management strategy that balances the benefits and risks and does not inhibit your ability to collaborate, attract international talent or create sustainable funding.

Consider the Risks

Ensure that there are policies and processes in place for identifying risks associated with research collaboration and that they have been communicated.

Ensure that those responsible for risk management decision-making are clear about the scope of their responsibility, have appropriate support and understand when decisions need to be escalated for more senior attention.



TRUSTED RESEARCH

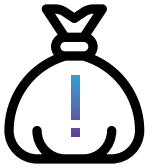
CONTRACT

Mitigate your Risks

Proportionate risk management will mitigate the risks to a level acceptable to your organisation.

Mitigations should be balanced and proportionate to the risk posed to the research you have identified as being critical or sensitive across your institution. Focus on protecting the research that is most sensitive, or which may pose reputational risk.

PATENT



Financial Risk

Have an institutional level view of the financial risk of over-reliance on single sources of funding, whether that may be from a single organisation or from a limited number of organisations from a single country.

This understanding will support the maintenance of a sustainable long-term funding model and will limit the ability of countries or organisations to infringe academic freedom or policy at your institution.

Legality

Have a clear understanding of the legal framework for international collaboration. This is essential to protect the integrity of the system of international collaboration.

Act in compliance with UK law, such as visa requirements, the Academic Technology Approval Scheme (ATAS), export control and data handling under the General Data Protection Regulation (GDPR).

Be aware that a range of academic activities, such as research on behalf of an international partner and overseas academic exchanges, fall within the scope of export control.

International Legal Frameworks

International collaborators must comply with their home country's laws. Ensure that processes and oversight take into account the local legal frameworks in which international research collaborators operate.

This could include laws and regulations that require organisations to share information and data with their state.

Protect your staff

Ensure that there are appropriate systems in place to support the recruitment and retention of international staff and visiting academics and students.

This could include supporting staff with appropriate visas and ensuring that they have suitable access to the institution's IT network and services. Consider providing training on their responsibilities to comply with relevant UK legislation and university policy.

Ensure that staff travelling overseas are briefed, trained and equipped to keep themselves and their sensitive information secure, and are aware of their responsibilities under export control and their contractual commitments to the university.

Take a proportionate approach to overseas travel advice that takes into account the laws and customs of the destination country. Where appropriate ensure that there is clear advice about taking and using IT equipment including removable media.

Manage access

Consider proportionate measures to ensure that staff, researchers, visiting academics and industry partners only have access to the buildings, information and networks that are necessary for their research and that there are added protections around sensitive areas of research.

Ensure that there is corporate oversight of who has access to your facilities and IT systems, including short-term academic visitors.

Much of the work of international research and collaboration happens online. Ensure that there is sufficient understanding of the security implications of the institutional support of any collaborative IT platforms, especially those used by third parties.

Protect your research and information

Understand how your information and cyber security policies support a **Trusted Research** approach.

This could include supporting your senior leadership through the NCSC Cyber Security Toolkit for Boards.

This will develop an understanding of the importance of measures such as segregating areas of your network that contain sensitive or valuable research.

Talk to your key industry partners and collaborators about how you are protecting their research and information.

Create a culture of Trusted Research

Lead by example. A **Trusted Research** culture relies on visible endorsement from the top. Consider running a **Trusted Research** campaign at your institution supported by training and regular communication with both research and corporate staff.

Focus on how you can support and encourage positive behaviour by including measures in your existing processes and procedures.

Consider identifying one or more individuals (ideally within both academia and corporate services) to champion the campaign. Ensure that all staff are clear about what to do if they have questions or concerns.

Build trusted relationships

Having a **Trusted Research** culture across your institution could be viewed as a key benefit by industry partners. Raise awareness of **Trusted Research** within your academic community and with your industry partners to demonstrate your institution's commitment to the security of research and the product of that research.

Ensure that you and your staff are clear on their commitments to avoid conflicts of interest and are aware of any contractual undertakings to which they must adhere.

Key questions for your institution

- Who is responsible for securing your research activities at senior leadership level?
- Do you have visibility of your institution's most important partners or funders, including those on which your institution is financially and reputationally dependent?
- Do you have a process for identifying and managing high-risk research collaboration?
- Are staff clear on when and to whom they ought to escalate high-risk research collaboration?
- Do you have confidence that your institution is compliant with export control, GDPR and other legal requirements?
- Do you have someone identified to champion the **Trusted Research** campaign in your organisation?

For more information and advice on **Trusted Research** visit ***www.cpni.gov.uk*** or ***www.ncsc.gov.uk***

Disclaimer

The information contained in this document is accurate as at the date it was created. It is intended as general guidance only and you should not rely on it.
This information should be adapted for use in the specific circumstances required and you should seek specialist independent professional advice where appropriate before taking any action based on it. To the fullest extent permitted by law, CPNI and NCSC accept no liability whatsoever for any loss or damage incurred or arising as a result of any error or omission in the guidance or arising from any person acting, relying upon or otherwise using the guidance. Full terms and conditions governing the use of this guidance are available on our website at www.cpni.gov.uk All references to CPNI in the Disclaimer section of those terms and conditions shall in respect of this guidance also include NCSC.

Freedom of Information Act (FOIA)

This information is supplied in confidence to the named reader and may not be disclosed further without prior approval from CPNI. This information is exempt from disclosure under the Freedom of Information Act 2000 (FOIA) and may be exempt under other UK information legislation.