Northeastern University
London

Trusted Research and knowledge exchange

What is ‘Trusted Research’?

Northeastern University London emphasises the importance of ‘Trusted Research’ – a concept endorsed by the UK government and the research and innovation sector. This term highlights the necessity of safeguarding the integrity of international collaboration, which is crucial for sustaining the momentum of research and innovation in the UK. The aim is to conduct safe, secure and transparent research whilst supporting the UK’s research integrity and strong ethical frameworks.

Trusted Research is particularly relevant for researchers involved in science, technology, engineering and mathematics (STEM) fields, dual-use technologies, emerging technologies, and areas of research that are commercially sensitive, **but everyone should be aware of the risks**.

Guidance on Trusted Research

Guidance on Trusted Research has been developed by the UK’s National Protective Security Authority in collaboration with the research and university community. Its purpose is to assist the UK's research and innovation sector in maximising the benefits of international scientific cooperation.

University staff have a duty to assess their work and partnerships, including collaborators and funders, and to recognise and address the risks of malicious interference. Therefore, they should familiarise themselves with the guidance available on the Trusted Research website.

The guidance covers:

- identifying potential risks and making well-informed decisions regarding them
- engaging in international collaborations confidently, securely, and safely
- safeguarding intellectual property, sensitive research, and personal information
- shielding research projects and staff from potential theft, misuse, and exploitation

How do I ensure my work adheres to ‘Trusted Research’ principles?

1. Trusted Research and knowledge exchange checklist
2. Export controls
3. National Security and Investment Act
4. International travel for research

Northeastern University
London

Trusted Research and knowledge exchange checklist

Partner due diligence

- Is there any information available to the public about an organisation or entity that might worry you?
- Does the collaboration or research partner raise any ethical or national security concerns?
- Is the potential partner connected to the military or government, especially from a country with different democratic and ethical standards?
- What do you know about the level of freedom and legal system in the country where your research partner operates?
- Could the partnership cause any conflicts of interest for you or the University?
- For visiting academics and students, do you know who employs them or funds their visit or studies?

If any of the above questions raise concern, or you are unsure of the answers, please contact RKE Services.

The below resources from NPSA Trusted Research could also help inform your decision about the suitability of research with specific partners:

- UN sanctions list
- Country corruption index
- Trade restrictions on export
- The Human Freedom Index
- The World Justice Project Rule of Law Index
- US Consolidated Screening List
- Consolidated Screening List search engine

Managing data and sharing information

- Are you providing any existing intellectual property (IP), research data or confidential information? If yes, how will you protect it?
- Are there sufficient information and cybersecurity measures in place within your research team?

- What level of access will the research partner have to your IT network, and what might this access reveal?
- Will the collaboration involve moving goods or transferring software, data or technology from the UK to a destination outside the UK? If so, does this fall under UK Export Control Regulations? Refer to the University's Export Control Policy.
- Are you sharing any information, goods or materials subject to other restrictions, such as US Export Control regulations? This includes any terms specified in funding or research agreements with third parties.

Intellectual property protection

- Will there be an agreement in place to safeguard the university's results, information and intellectual property involved in the collaboration?
- Does the collaboration allow for the free publication of results and uphold academic freedom without interference?
- Can the project be separated from other research projects, including those with third-party involvement or funding?
- Will access to information and results be limited to what is necessary for the collaborator (including visitors) to carry out the project?
- Are suitable information and cybersecurity measures implemented within your research group?

Contact research@nulondon.ac.uk to request for an agreement to be drafted or a partner agreement to be reviewed.

National Security and Investment Act (NSI)

What is the NSI?

The National Security and Investment Act (NSI Act) became effective on 4th January 2022. This legislation empowers the government to scrutinise and intervene in specific acquisitions by individuals or organisations if they pose a threat to the UK's national security. The government can impose conditions on acquisitions and, if necessary, prevent or reverse them.

Universities and research institutions should consider the NSI Act when engaging in collaborations involving the acquisition, sale or development of certain entities and assets, known as qualifying entities and assets. The government has authority to evaluate acquisitions at any stage – whether completed, ongoing or under consideration – if there is reasonable suspicion of a national security risk.

What kind of operations are covered by the NSI Act?

The NSI act requires you to notify the government if you are acquiring entities or assets in one of 17 areas of the economy deemed sensitive to national security:

- advanced materials
- advanced robotics
- artificial intelligence
- civil nuclear
- communications
- computing hardware
- critical suppliers to government
- cryptographic authentication
- data infrastructure
- defence
- energy
- military and dual use
- quantum technologies
- satellite and space technologies

- suppliers to the emergency services
- synthetic biology
- transport

Examples of qualifying entities and assets in higher education

Entities	**Assets**
University that is registered as a charitable organisation	Designs
Private university	Software
Trust	Land
University spin-out	Trade secrets
Research organisation	Source code
Private company or corporation doing contractual work with a higher education institution or research organisation	Algorithms and formulae
University subsidiary (eg a company that a university has incorporated and carries out specific activities that the university operates)	Plans, drawings and specifications
	Land and tangible moveable Property, eg laboratory equipment

Examples within a higher education context

Example 1

A company sponsors a professorship in a UK university. The company can influence the direction of the research the professor leads but has no agreed access to any Assets.

This scenario is not a qualifying acquisition and not in scope of the NSI Act as the company has not gained control over any qualifying entity or asset.

Example 2

A foreign corporation provides funding for a UK university to carry out a research project on the foreign corporation's behalf. The foreign corporation sits on the steering board for the research project. The foreign corporation will also be entitled to all intellectual and tangible moveable property generated from the research.

The government may be able to call in this contemplated acquisition for assessment if it reasonably suspects the acquisition may give rise to a risk to national security. This is because this scenario is a contemplated qualifying asset acquisition, as the funding gives the corporation control over any intellectual or tangible moveable property generated through this project.

You are not legally required to notify the government in this scenario as the research project is not a qualifying entity, and mandatory notification only applies to certain acquisitions of qualifying entities.

Example 3

A private foreign company funds an employee through an academic placement which results in a PhD. As part of the employee's contract, all intellectual property generated is assigned to the company.

The government may be able to call in this contemplated acquisition for assessment if it reasonably suspects the acquisition may give rise to a risk to national security. This is because this scenario is a contemplated acquisition of control over a qualifying asset as the private company has contractual rights over any intellectual property generated by the employee during their PhD.

You are not legally required to notify the government in this scenario as no party has acquired a qualifying entity, and mandatory notification only applies to certain acquisitions of qualifying entities.

Further reading

The National Security and Investment Act: guidance for universities - Universities UK

International travel for research

What to consider

If you're travelling to higher-risk countries, then you may need to be prepared for a different experience. For example, people visiting hostile nation states have reported a range of security issues, such as:

- restricted access to popular services (including Gmail, Wikipedia and social media sites)
- government monitoring of communication services such as Skype
- unreliable and untrustworthy WiFi connections
- restricted use of VPN
- hotel staff and government officials accessing devices left in hotel rooms.

You should always check the UK foreign office advice before travelling. Please see the information relating to travel and insurance in the links below and in the company documents on PeopleHR.

Please remind yourself of the travel and spending guidelines when you are preparing for a business-related trip and read through the global support resources for travel presentation.

Authorisation of travel

When travelling for work, you should register your university business trip with Global Safety and Support. Travel must also be logged with HR on Workday.

Currently, all travel (international and domestic) must be approved by Boston. Please speak to your faculty director about this in the first instance.

Compliance with export control regulations while overseas

- Staff and PGR students involved in research with international partners must inform their RKE Services in advance of any travel or work outside the UK to receive necessary support and advice.
- University staff must not take controlled/end-use data out of the UK without the appropriate export licence.
- Electronic devices containing controlled data must not be taken overseas without the relevant export licence.

- If electronic devices contain controlled data, request a blank device from IT or remove all controlled information from the current device before travelling.
- Do not use university shared drives or other university servers to access controlled information while overseas.