

**TRUSTED  
RESEARCH**

---

# Implementation – scenarios



National Protective  
Security Authority



National Cyber  
Security Centre



## Contents

<b>Scenario 1:</b> Authoritarian government	<b>4</b>
<b>Scenario 2:</b> Overseas presentation and government approach	<b>10</b>
<b>Scenario 3:</b> Hosting sensitive data overseas	<b>16</b>
<b>Scenario 4:</b> Talent plan, funding conflicts and changing research scope	<b>22</b>
<b>Scenario 5:</b> University spin-out	<b>28</b>
<b>Scenario 6:</b> Identifying export controls and sanctions	<b>34</b>
<b>Scenario 7:</b> Identifying dual-use applications before commercialisation	<b>38</b>



# Scenario 1: Authoritarian government



W was a post-doctoral research associate focused on photonics research at a UK university. They had moved from their home country, an overseas country with an authoritarian government, to the UK for this role.

While employed by the UK university, they **travelled overseas** to their home country on **university-related business**. During the trip, they were **instructed by the authoritarian government** in their home country that they would not be returning to the UK.

W did not contact the UK university to formally end their employment.

During a routine scan of the university network two weeks after W left the UK, the UK university IT team identified **remote downloads from a server linked to the photonics department to an overseas server**. The downloads involved significant amounts of sensitive research data that W had been working on. Further investigation identified that **W's credentials had been used to access the network** at the time of the download.

It was later established that W now **worked in direct collaboration with the military** of their home country on similar research to that which they undertook in the UK.

## Considerations

Universities should be aware of **other countries' legislation**, which may require individuals to co-operate or compel them to share research data with foreign governments or intelligence services (e.g. export control or national security legislation which may have extra-territorial reach).

Universities should also consider the geopolitical climate associated with an overseas partner, for example involvement of the state in military action or strained diplomatic relations, that may heighten risks to individuals when travelling or the existence of an autocratic or authoritarian government.

Overseas legislation and political actions which may put the traveller at increased risk should be factored into **insurance considerations** and captured in a **pre-travel risk assessment**.

In this scenario, W may have:

- been placed under **duress** by an overseas government to cooperate
- **willingly** co-operated with an overseas government
- **naively**, but purposely, passed sensitive information to an overseas government
- been victim of a **cyber attack** in which their credentials and university network access were breached

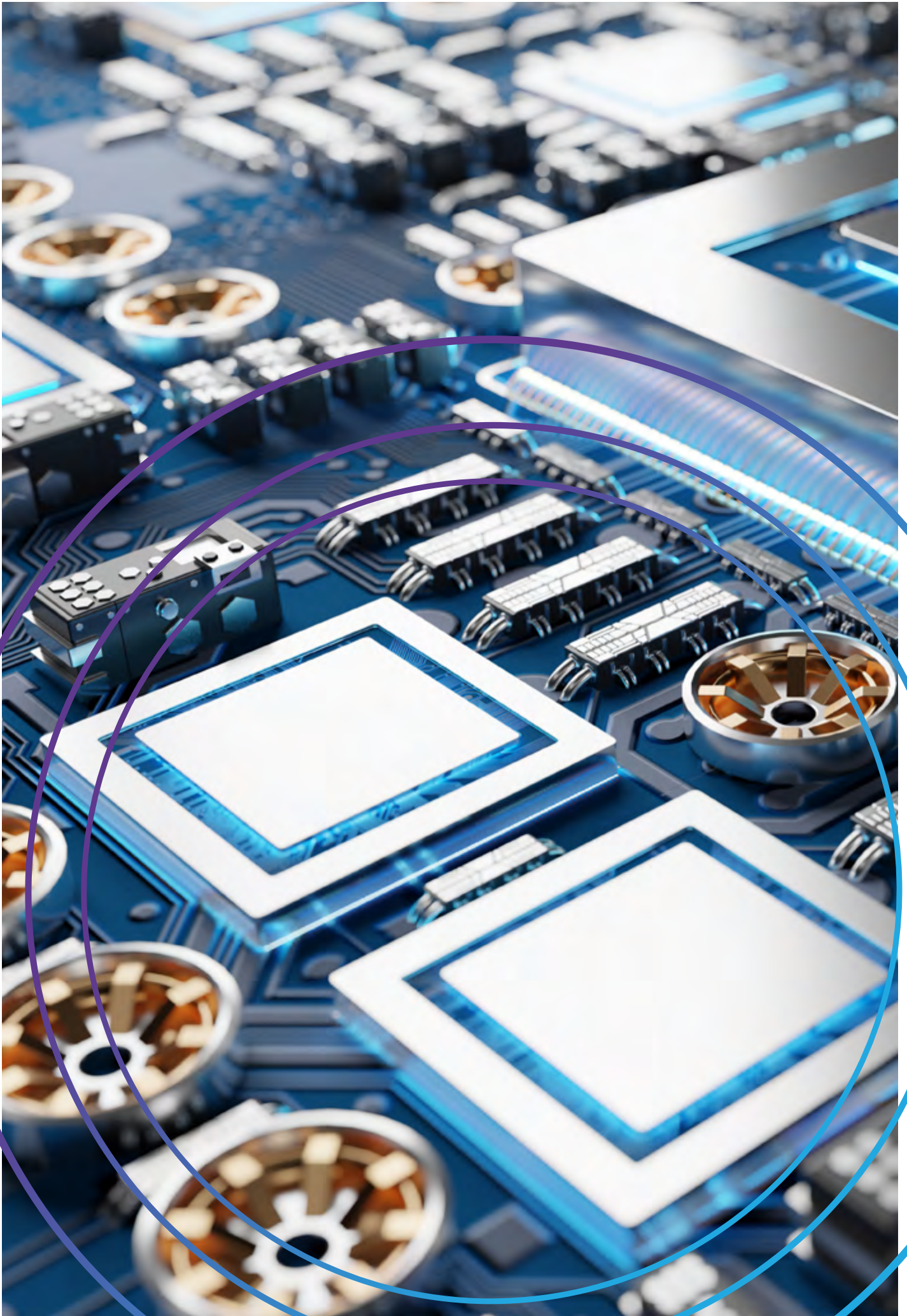
The considerations and mitigations will vary depending on the circumstances, but the following may be applicable.

- Universities will include a range of conditions and undertakings in academic contracts, and in most cases will retain **ownership of research** conducted while employed by the university. While research associates may consider themselves the sole owner of any research that they undertake, the university at which they are employed may view themselves as the owner as they employed the academics involved and provide the resources to facilitate the research.
- **Access to IT systems** should be governed by clear policies that include considerations for overseas access, downloading materials from university systems and their onward dissemination and employee monitoring.
- **Access credentials**, such as passwords, should always be unique and complex to prevent opportunistic guessing. They should always be stored safely.
- Unauthorised interference and theft of data without permission from a university network could constitute a criminal offense under the **Computer Misuse Act (CMA)**.
- Depending on the circumstances, it is possible that the download of research data from a UK university to an overseas university could place the researcher in breach of **export control**, and in some cases the **Data Protection Act 2018**.
- Depending on the circumstances, the **National Security Act 2023** could be relevant. For example, in the instance of sharing trade secrets.

## Institutional mitigations

To mitigate the risks, institutions may want to consider:

- **conducting risk assessments** to identify any country-specific risks and any risk factors which may make their staff vulnerable
- providing **guidance to staff travelling overseas**, particularly to countries in which staff may be subjected to unwanted or uneasy approaches and/or government pressure
- implementing reporting mechanisms for staff travelling overseas to be able to **report concerns and incidents** to their institution (e.g. uneasy approaches, cyber attack, theft, being followed etc.)
- providing a **'helpline'** (or equivalent system), which staff can use discreetly to flag that they are under duress
  - Institutions may wish to build additional functionality into such processes, for example temporary suspension of all university network access.
- **restricting access to their internal network** and associated file structures for those visiting countries which are perceived as 'higher risk', regarding technology transfer and IP theft, according to institutional risk thresholds
- facilitating the option for staff, and students where necessary, to take **'clean' devices** overseas which contain only the information required for the trip
- communicating clear expectations and contractual requirements relating to the **ownership of research** and the sharing of intellectual property
- **removing physical** (e.g. laboratory/office access, scientific samples, hardcopy files/data etc.) **and IT accesses** (e.g. university networks and file structures, email accounts etc.) immediately as part of institutional exit procedures to prevent access to sensitive data and intellectual property after the end of employment
  - Institutions may wish to automatically engage exit procedures, or temporarily suspend accesses, during periods of non-contact from employees.
- offering support for **personal travel on a voluntary basis** if staff, and students where relevant, feel it is necessary






## Individual researcher mitigations

To mitigate the risks, with guidance from the research office, academics/researchers may want to consider:

- familiarising themselves with the **local laws and customs** of their destination, as well as any political circumstances that may be cause for concern prior to travelling
  - familiarising themselves with the **institution’s travel policies/processes**, particularly regarding accessing data
  - identifying institutional **reporting mechanisms**, in case you require assistance while overseas
  - understanding the institution’s contractual expectations regarding the **ownership and sharing of IP** developed while employed by the university, both during and at the end of their employment, to avoid contractual breaches when engaging with partners
  - that accessing controlled data or intellectual property from UK university servers while overseas may constitute a breach of **export control** – this applies regardless of whether you are accessing information for the purposes of sharing it or accessing information solely for independent work
- Breaches of export control can result in financial penalties, reputational damage, loss of funding and imprisonment. It is important to maintain awareness of this.
    - Either the individual or institution or both could be liable to prosecution, depending on the circumstances including the degree of involvement.
    - You can use the **Goods and Open General Export Licenses (OGEL) checker** to check whether the items you want to export are regulated by export controls and to determine if an Open License is available for your scenario. For advice on obtaining export control licenses, you should contact your university research office and/or HMG’S Export Control Joint Unit (ECJU).



# **Scenario 2: Overseas presentation and government approach**

B is a Professor of **advanced materials** at a UK university and receives **funding from a UK defence industry partner**.

Professor B has been corresponding with Professor Y for six months on an area of shared academic research interest. Professor Y is based at an **overseas university** in Country Z and invited Professor B there to give a lecture to a group of students and post-doctoral researchers on advanced materials. Professor B accepted the invite and travelled overseas to give the presentation.

Following the presentation, several **additional people joined the question-and-answer session**. The questions focused on potential aerospace applications of advanced materials and there were a few questions about Professor B's work with the UK defence industry partner.

On the second day of the visit, Professor Y introduced Professor B to a member of the Science Ministry of the **government** for Country Z.

Although they were not able to discuss the specifics of Professor B's research, due to the existence of a **non-disclosure agreement** (NDA) with the UK defence industry partner, the government representative discussed their desire to **replicate the research facilities** that Professor B used in the UK.

They also discussed their wish to use them to **pursue similar research** to that which Professor B undertook with the UK defence industry partner.

The government representative was interested in exploring whether Professor B would act as a **consultant to the overseas government** in establishing the research facility and asked if Professor B would visit again to discuss this in more detail. The Science Ministry representative offered to pay Professor B's **travel expenses and compensate** them for the work.

Professor B agreed to act as a consultant for Country Z's Science Ministry and **accepted a payment of £5,000.00** as an initial retainer.

Upon returning to the UK, Professor B was contacted by the Export Control Joint Unit (ECJU) at the Department for Business and Trade. The ECJU had been made aware of the lecture that Professor B provided abroad and were concerned about whether any of the material that was shared was subject to export control.

## Considerations

Considerations may vary slightly depending on which overseas country is involved in this type of scenario.

**Presentations and lectures given overseas**, or online in the UK to an overseas audience, may be subject to export control.<sup>1</sup> Given that Professor B was undertaking defence related research, their work was likely to be considered sensitive research.

When travelling overseas with devices, individuals **must consider all the information held on their devices** and whether any of it is subject to export control – this is necessary regardless of whether you plan to share the information with individuals while overseas. In many instances, it is easier to take a ‘clean’ device which contains only the information required for the trip.

Disentangling export controlled and non-controlled materials can be particularly difficult if your institution promotes a ‘bring your own device’ culture, in which your device is both your personal and work device.

In ‘bring your own device’ situations, consideration regarding export control will need to be taken for all overseas trips, including travel for leisure and holidays.

The **funding** from the UK defence industry partner was likely subject to **terms and conditions**, or **contractual obligations**. For example, there may have been a requirement to alert the partner of other engagements which may impact on their research area. In addition, accepting payment from an overseas government to replicate the work was likely a conflict of interest/commitment.

If accepting **payment or expenses** from an additional organisation, you should consider whether you need to **declare** them to your institution, existing partners/funders and/or HMRC.

The Trusted Research Countries and Conferences Guidance<sup>2</sup> provides additional advice on overseas travel.

1 <https://www.gov.uk/guidance/export-controls-applying-to-academic-research#basic-scientific-research>

2 <https://www.npsa.gov.uk/system/files/Countries%20and%20Conferences%20Guide.pdf>



## Institutional mitigations


To mitigate the risks, institutions may want to consider:

- putting effective **travel policies/processes** and incident **reporting mechanisms** in place to support their staff when travelling overseas
  - Institutions may wish to use reporting mechanisms as a means to identify patterns in incidents which can be communicated to staff, and students where relevant, to increase their awareness of risks while travelling. This data can also be used to inform risk thresholds and policy changes.
- recommending that staff, and students where relevant, take **‘clean’ devices** when travelling overseas and resourcing this process
- providing **guidance** to those travelling to **‘higher risk’ countries** in which they may be subjected to approaches that could incur risks
  - This guidance will be governed by institution’s risk thresholds.
- helping researchers/academics to understand the **terms and conditions/contractual obligations** that govern their employment, funding, intellectual property ownership and legal compliance obligations
- adopting policies/processes which encourage researchers/academics to **disclose payments** they accept through private consultancy (or equivalent)
  - The intention of this is to safeguard the academic institution against any potential accusations of non-compliant collaboration.

## Individual researcher mitigations

To mitigate the risks, with guidance from the research office, academics/researchers may want to consider:

- with the assistance of the research office, conducting **open-source research on partners** to help identify any potential risks, for example links to an overseas military
- familiarising themselves with the **local laws and customs** of their destination, as well as any political circumstances that may be cause for concern prior to travelling
- familiarising themselves with the **institution's travel policies/processes**, particularly regarding taking devices overseas
- identifying institutional **reporting mechanisms** in case you require assistance while overseas
- seeking advice from the research office to establish whether an **export license** is required to ensure legal obligations are met
- discussing any terms and conditions/contractual obligations you must uphold with the research office to ensure they are fully understood

A futuristic white robot hand with glowing joints is shown typing on a laptop keyboard. The robot's hand is positioned over the keyboard, with its fingers pressing down on the keys. The background is dark with bokeh light effects, suggesting a high-tech or digital environment. The robot's hand is illuminated with a bright yellow light, and the keyboard keys are also lit up. The overall scene conveys a sense of advanced technology and data processing.

## **Scenario 3: Hosting sensitive data overseas**



G is a post doctorate researcher specialising in **artificial intelligence (AI)** and has been corresponding with Professor B at an **overseas university** for six months on a shared area of research interest.

G is being **funded by a UK police force** to undertake research into the use of AI for the identification of criminality and terrorism based on CCTV coverage. Professor B has been undertaking similar research with a police force in their own country. Subsequently, G and Professor B agree to share research developments and data.

Professor B suggests that the research is **hosted on a new IT platform developed by the overseas university**. G is impressed by the functionality of the IT platform and agrees to hosting the research on the platform, which includes **bulk personal data** provided by the UK police force.

A few weeks later, a national newspaper in the UK publishes an article about the collaboration between the UK and overseas university. The article alleges that the overseas university provided the overseas police force with AI technology, developed in collaboration with the UK university, to conduct widescale **surveillance on a minority group** to

support a regime of repression and ill treatment.

As a result of the collaboration, the UK university's reputation is damaged and they face widespread criticism. G attempts to access the overseas university's IT platform to remove the bulk personal data provided by the UK police force but is **denied access**. G consults their institutional data security policy and reports the incident to the internal IT team.

Due to the breach of data security, the UK police force **withdraw funding** from multiple projects with the UK university.

## Considerations

Considerations may vary slightly depending on which overseas country is involved in this type of scenario.

Under the National Security and Investment Act 2021 (NSI Act), the UK government may call in a **qualifying acquisition of an asset**<sup>3</sup> if they have reasonable suspicion that it has given rise to, or may give rise to, a risk to national security. Universities and other research-intensive organisations may make a voluntary NSI notification about an acquisition if they wish to be certain whether the acquisition will be called in.

This power is more likely to be used for qualifying acquisitions of assets that are, or could be, used in connection with the activities set out under the **17 sensitive areas of the economy**<sup>4</sup> or closely linked activities. This is because these acquisitions are more likely to pose a risk to national security. In this instance, as AI is one of the 17 sensitive areas of the UK economy and databases are included as qualifying assets, a voluntary notification could have been submitted to the UK government.

Given the sensitive nature of the research and the use of **bulk personal data**, there are implications to consider in relation to the **Data Protection Act 2018**, particularly due to the use of an IT platform hosted outside of the UK. If personal data collected by visual surveillance technology is sent to another jurisdiction, the Data Protection Act 2018 requires assurances that data protection legislation in that jurisdiction is essentially equivalent to that in the UK.

**The transfer of knowledge overseas may be subject to export control.**

As the research was focused on AI and has a clear dual-use application, it is essential to secure the relevant export control license before exchanging knowledge and sending data to be hosted on an overseas IT platform.

Recipients of funding have a responsibility to ensure that they are **compliant with the terms and conditions of the funding** and are aware of their **responsibility to conduct due diligence** on the source of funding and partners. This includes new members to existing partnerships and additional streams of funding introduced during the project, where relevant.

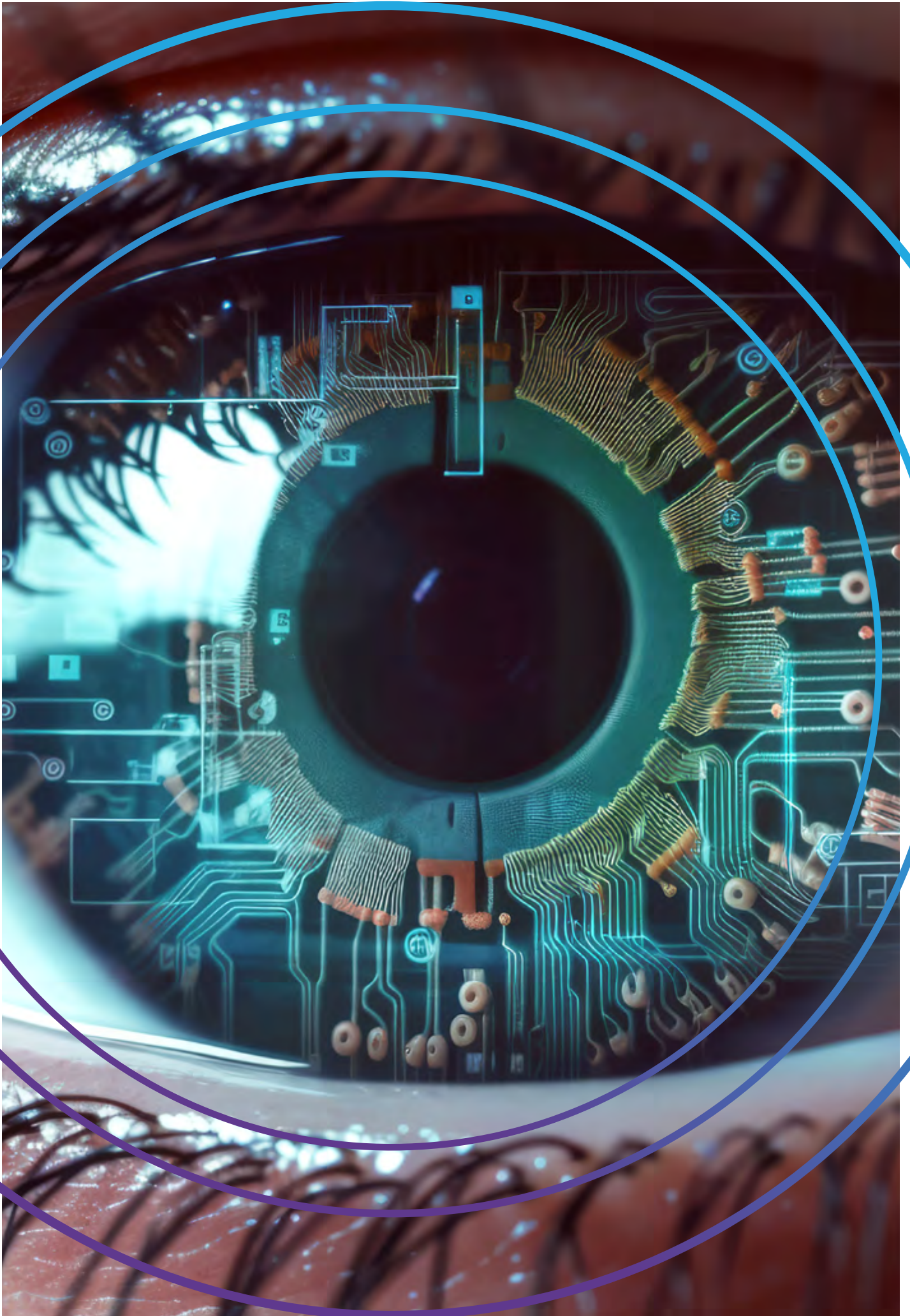
3 <https://www.gov.uk/government/publications/national-security-and-investment-act-guidance-for-the-higher-education-and-research-intensive-sectors/national-security-and-investment-act-guidance-for-the-higher-education-and-research-intensive-sectors#how-the-rules-work>

4 <https://www.gov.uk/government/publications/national-security-and-investment-act-guidance-on-notifiable-acquisitions>

## Institutional mitigations

To mitigate the risks, institutions may want to consider:

- providing **training** on the Data Protection Act 2018 and all other relevant legislation
- using a **data security policy** to govern where and how sensitive information/data should be stored and handled –the policy should:
  - encourage researchers to use the institution’s internal IT network for sensitive data to ensure they remain the controller of the information/data
  - state the necessity of using appropriate storage locations e.g. suitable for bulk personal data
  - outline the process for reporting incidents/breaches
  - promote a ‘no blame’ culture which encourages staff to engage with the reporting process
  - recommend that data is backed-up in an appropriate and secure location to protect against loss
  - be usable for the various kinds of data the institution needs to protect
  - create data management plans for collaborations, where relevant, which include security considerations



## Individual researcher mitigations

To mitigate the risks, with guidance from the research office, academics/researchers may want to consider:

- conducting **open-source research** on partners and their funding sources
- familiarising themselves with the **terms and conditions** attached to any information/data they are given
- these terms and conditions should have defined acceptable methods and locations for the processing, storing and transportation of the data.
- **hosting research data** within their own institution to enable a **higher degree of control and monitoring** of the information to ensure it is adequately protected, where possible

**Scenario 4:  
Talent plan, funding  
conflicts and changing  
research scope**



T is a research fellow at a UK university receiving government funding for conducting research on **genome editing** for the purposes of **developing new medicines**. T recently published multiple academic papers on their research and subsequently received a message from a senior employee at a **UK subsidiary of a synthetic biology (SynBio) company** headquartered overseas (Company A).

The senior employee showed significant interest in T's research and requested a meeting in person. During the meeting, the senior employee presented an offer from Company A to provide T with **additional funding and lab space** at their facility in the UK. The overseas senior employee stated that this would be an **informal talent plan arrangement** and that as such, it would not be necessary for T to inform their university of the collaboration.

T accepted the offer and continued their research on genome editing for the development of new medicines, simultaneously working at the university research facilities and at Company A's facility.

T found the staff at Company A very friendly, they frequently invited T to networking events and suggested that T bring colleagues from the UK university. Over the course of 3 months, **T introduced Company A to numerous academics** from the UK

university and provided the contact details of additional colleagues at Company A's request.

After working with Company A for 3 months, T's government funding partner requested to meet with them. The funder had become aware that T had received an **additional stream of funding** for the project that they had also been funding. This conflicted with the terms and conditions. As a result, the government partner **withdrew their funding**.

A few weeks after T's government funding was withdrawn, Company A offered T **additional funding** to work on a research project using SynBio to **enhance physical and cognitive human performance**. T agreed to work on the project.

## Considerations

Institutions and researchers/academics should be aware of the **ultimate beneficiary** of their work. If you are working with a UK subsidiary of an overseas company, it may be necessary to **explore the structure of the organisation** to conduct sufficient due diligence. Depending on how information is transferred through that structure, you may also need to consider whether export controls apply.

A reliable research partner should have **no reason to hide their current or previous affiliations** from you or your employer, nor should they request you to do so.

Legitimate collaborations are typically formalised by **contracts**, and it should be viewed as a red flag if a partner insists that a contract is not required.

Foreign talent plans often incentivise their members to **recruit their existing partners and colleagues**, creating a domino effect whereby greater and greater amounts of research and intellectual property is transferred.

**Due diligence is an ongoing process** which should be revisited when changes take place during the lifecycle of a collaboration. For example, a change in research scope, funding source or new individuals being introduced to an existing partnership.

Under the National Security and Investment Act 2021 (NSI Act), the UK government may call in a **qualifying acquisition of an asset**<sup>5</sup> if they have reasonable suspicion that it has given rise to or may give rise to a risk to national security.

Universities and other research-intensive organisations may make a voluntary NSI notification about an acquisition if they wish to be certain whether the acquisition will be called in. This power is more likely to be used for qualifying acquisitions of assets that are, or could be, used in connection with the activities set out under the **17 sensitive areas of the economy**,<sup>6</sup> in which synthetic biology is included, or closely linked activities. This is because these acquisitions are more likely to pose a risk to national security.

Institutions should ensure that they **educate and protect** their most **vulnerable staff and students** from potentially exploitative approaches. Staff and students may be more vulnerable at the start of their careers, when they may have less experience managing research security risks, or if they are on insecure or short contracts in which they need to meet funding targets.

5 <https://www.gov.uk/government/publications/national-security-and-investment-act-guidance-for-the-higher-education-and-research-intensive-sectors/national-security-and-investment-act-guidance-for-the-higher-education-and-research-intensive-sectors#how-the-rules-work>

6 <https://www.gov.uk/government/publications/national-security-and-investment-act-guidance-on-notifiable-acquisitions>





## Institutional mitigations

To mitigate the risks, institutions may want to consider:

- defining what constitutes a **formal collaboration**, for instance, one in which funding and/or facilities are provided, and therefore requires **reporting to the university**
- providing staff, and students where necessary, with **training** on the NSI Act
- briefing staff, and students where necessary, on **research security risks** and **approaches used by state actors** to target academia (e.g. talent plans)
- implementing **reporting mechanisms** for staff to be able to **report concerns and incidents** to their institution (e.g. uneasy approaches)

## Individual researcher mitigations

To mitigate the risks, with guidance from the research office, academics/researchers may want to consider:

- checking the **terms and conditions of existing funding** contracts before accepting additional sources of funding to ensure you are not breaching the terms and conditions
- **notifying your institution of collaborations** you are undertaking, in line with the relevant policies/processes
- conducting **open-source research** on partners and their funding sources
- considering the **wider possible applications of your research**. For example, dual-use applications
- **maintaining awareness of changes in the scope** of a research project which may require additional consultation with the research office regarding due diligence and legal obligations

# Scenario 5: University spin-out



J is a research associate at a UK university who developed a **drone** with capabilities to facilitate the mapping of endangered species in extreme weather conditions.

J was approached by a **UK-based subsidiary of an overseas technology company**, Company C, to commercialise the drone through the formation of a **university spin-out company**. The overseas technology company offered to oversee the business planning, manufacturing and sales to allow J to continue to develop further iterations of the technology.

Company C stated that they intended to market the drone primarily to producers of wildlife, travel and extreme sports documentaries. J was aware of the **dual-use applications** of the technology. For example, the drone had the ability to locate and track people, as well as animals. It was also fitted with high-specification lenses capable of withstanding explosions to maintain full functionality in adverse weather. As a result of these dual-use applications, J conducted **open-source research** on Company C and felt confident that they intended to use the technology for civilian purposes only.

In conjunction with the institution's technology transfer office (TTO), J went ahead with forming the university spin-out with Company C, which involved providing them with **exclusive licensing rights**.

A year after the formation of the spin-out, while J was conducting research to further develop the drone capability, J identified that the country in which Company C was headquartered had developed a **military drone** over the last 8 months. The military drone had multiple **identical capabilities** to J's drone and was almost identical in appearance.

J approached Company C, but they denied any involvement in the development of a military drone. At the end of the licensing period, Company C did not renew the agreement with J's university spin-out.

## Considerations

There is often an expectation that the researcher/academic's university will want to be a shareholder in any university spin-out companies established. The institution may have a specific **policy on university spin-outs**, particularly in regard to **IP ownership**.

Under the National Security and Investment Act 2021 (NSI Act), the UK government may call in a **qualifying acquisition of an asset**<sup>7</sup> if they have reasonable suspicion that it has given rise to or may give rise to a risk to national security. Universities and other research-intensive organisations may make a voluntary NSI notification about an acquisition if they wish to be certain whether the acquisition will be called in. This power is more likely to be used for qualifying acquisitions of assets that are, or could be, used in connection with the activities set out under the **17 sensitive areas of the economy**<sup>8</sup> or closely linked activities. This is because these acquisitions are more likely to pose a risk to national security. Drones would be included within the 'military and dual-use' sensitive area of the UK economy.

Consequently, Company C's investment into the university spin-out could have been voluntarily notified to the UK government.

Institutions and researchers/academics should be aware of the **ultimate beneficiary** of their work. If you are working with a UK subsidiary of an overseas company, it may be necessary to **explore the structure of the organisation** to conduct sufficient due diligence. Depending on how information is transferred through that structure, you may also need to consider whether export controls apply.

When working with overseas partners or in overseas markets, it may be necessary to obtain **additional IP protections**. However, some overseas territories do not uphold IP protections with the same rigour as the UK.

NPSA's Secure Innovation<sup>9</sup> campaign provides guidance on how to protect start-ups and spin-outs from state threats.

7 <https://www.gov.uk/government/publications/national-security-and-investment-act-guidance-for-the-higher-education-and-research-intensive-sectors/national-security-and-investment-act-guidance-for-the-higher-education-and-research-intensive-sectors#how-the-rules-work>

8 <https://www.gov.uk/government/publications/national-security-and-investment-act-guidance-on-notifiable-acquisitions>

9 <https://www.npsa.gov.uk/secure-innovation/company-guidance#security-from-the-start>

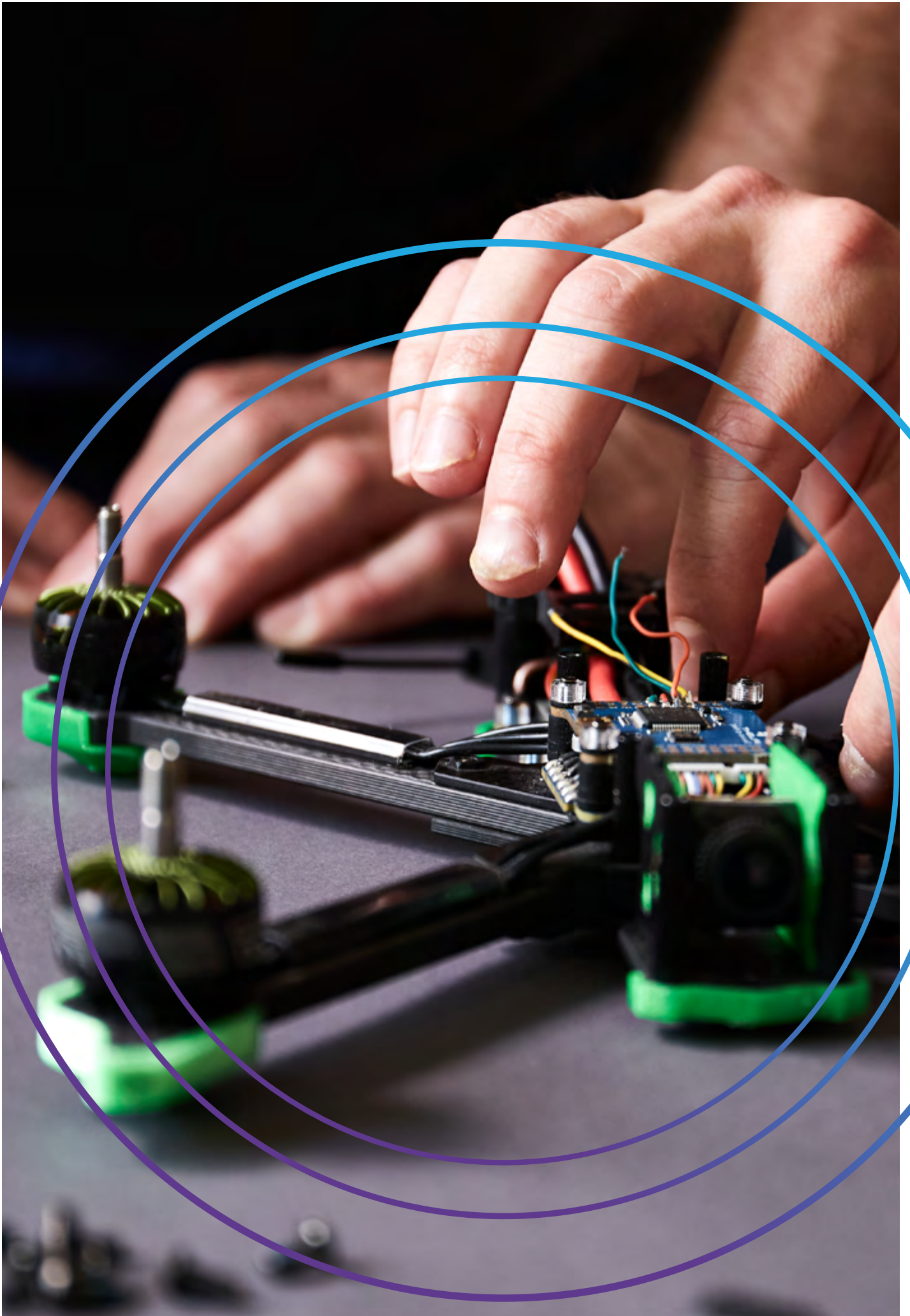
## Institutional mitigations

To mitigate the risks, institutions may want to consider:

- **providing training** on the National Security Investment Act (NSI Act), as well as the other legal obligations that researchers and academics must comply with – for example, the Academic Technology Approval Scheme (ATAS), export control etc.
- making use of the **Intellectual Property Office’s (IPO) range of training tools**<sup>10</sup> to help academics understand how to identify, protect, manage and leverage IP – there is also specific guidance<sup>11</sup> on dealing with sensitive patents

10 <https://www.ipo.gov.uk/ip-support/welcome>

11 <https://www.gov.uk/guidance/national-security-checks-on-patent-applications>






## Individual researcher mitigations

To mitigate the risks, with guidance from the research office and/or technology transfer office (TTO), researchers/academics may want to consider:

- conducting **open-source research** on partners and their funding sources
- identifying any **legal obligations** overseas partners, and their funders, may be subject to
- identifying the **legal owner of intellectual property** that is developed while employed by a university, before entering into contracts with external bodies
- This process will typically be overseen by the TTO.
- **seeking advice on IP protections**, both in the UK and in the relevant overseas jurisdiction(s)
- consulting institutional **policies on holding external appointments, conflicts of interests and IP ownership** prior to becoming involved in university spin-outs



# Scenario 6: Identifying export controls and sanctions



P was a PhD student at an overseas university conducting research on **advanced materials**. After finishing their PhD, P successfully applied for a postdoctoral research associate position at a UK university to conduct research into graphene.

While in the UK, P conducted extensive research into the application of **graphene as a protective material**. In their home country, P's former PhD supervisor was an expert in the application of graphene as a construction material. P wanted to collaborate with their former PhD supervisor on research into the structural composition of graphene.

P contacted their former PhD supervisor and asked if they would be willing to co-operate. They were keen to be involved and suggested that to fully understand the requirements of the UK research project, P would need to share the aims of the research project and the research which had been conducted thus far.

Before exchanging any research with their former PhD supervisor, who was based in their home country, **P consulted the UK university's policy/process on collaborations** which advised checking UK Government advice on **export controls and sanctions**. P consulted their research office for advice on undertaking these research security checks. With the assistance of their research office, P identified that their research would be **subject to export control due to the potential dual-use application** of graphene as a protective material and that their former PhD supervisor's **university was subject to UK sanctions**.

Through discussions with the research office, P recognised that it would not be possible to undertake the collaboration with their former PhD supervisor and **informed the UK university** that although they had been in contact with a sanctioned university, that the research into graphene as a protective material would not be discussed any further and no intellectual property had been transferred.

## **Considerations**

To mitigate risks, universities may want to consider putting **reporting mechanisms** in place for academics to be able to report interactions which may be of concern. To increase the likelihood of these functions being appropriately used, universities should aim to foster a **culture of transparency** so that reporting is seen as positive. In this instance, the interaction was halted before it became problematic but because P reported the interaction to the university, the institution could create a record of the exact circumstances which may be useful if any allegations of a collaboration are made in the future.

The use of graphene as a protective material falls under the Export Control Order 2008 (Schedule 2 – military goods, software and technology) and use of graphene in body armour (i.e. a protective material) would also fall under ‘Category 1 – special materials and related equipment’ of the UK Government consolidated list of strategic military and dual-use items requiring export authorisation.

You may want to use **the Department for Business and Trade’s Goods Checker tools**<sup>12</sup> to identify whether technology is subject to export control. This resource may provide a helpful indication of whether an export license is required but as it is primarily designed for goods, rather than research, it is always beneficial to **discuss your requirements with the research office**.

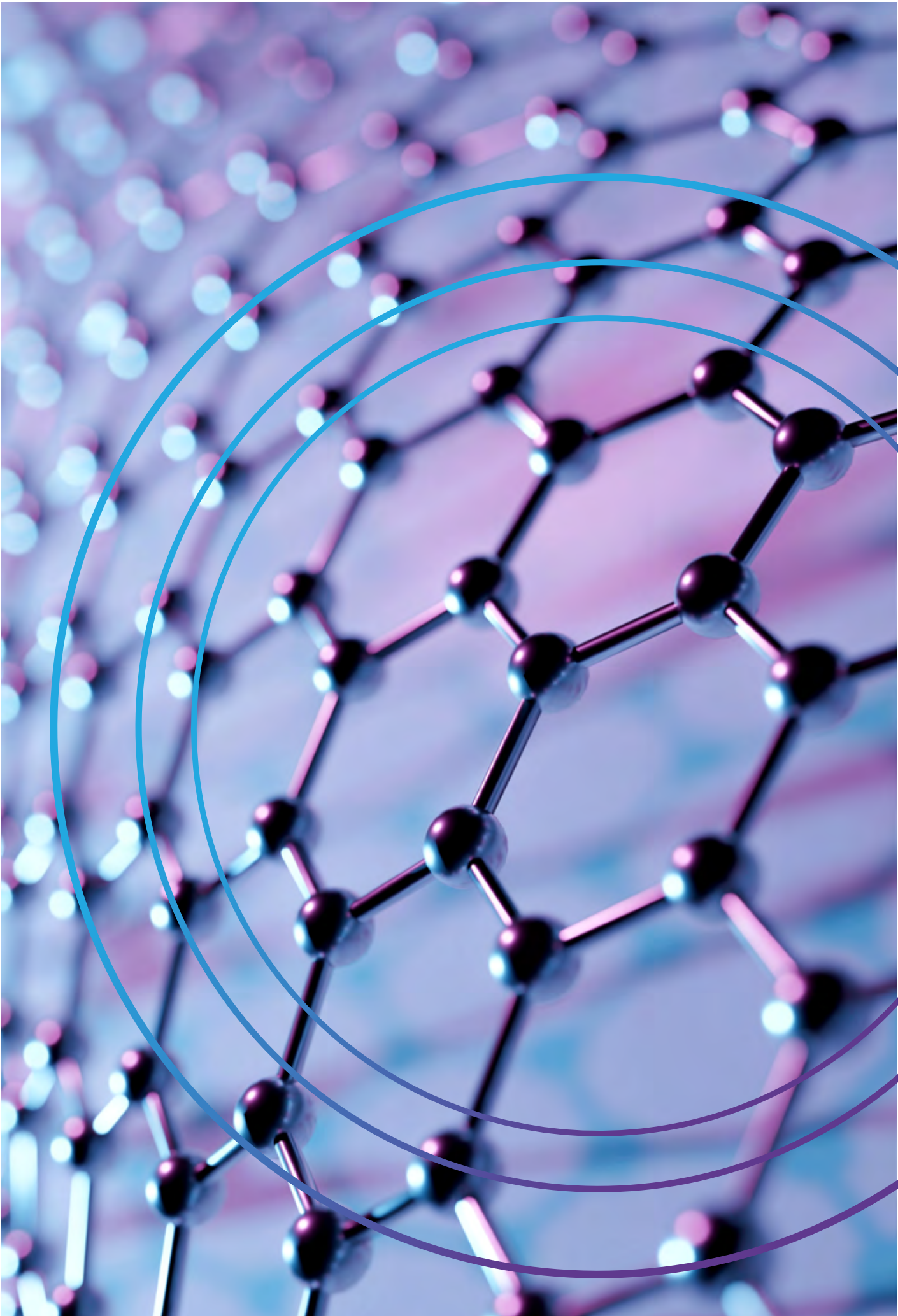
The UK Government can impose a variety of sanctions on individuals, organisations or countries. As such, there are a variety of different **sanctions lists**<sup>13</sup> **which must be consulted** prior to the transfer of goods, technology or knowledge.


Institutions should be alert to the use of third-party countries in international collaborations to circumvent UK sanctions.<sup>14</sup>

12 [https://www.ecochecker.trade.gov.uk/spirefox5live/fox/spire/OGEL\\_GOODS\\_CHECKER\\_LANDING\\_PAGE/new](https://www.ecochecker.trade.gov.uk/spirefox5live/fox/spire/OGEL_GOODS_CHECKER_LANDING_PAGE/new)

13 <https://www.gov.uk/government/publications/the-uk-sanctions-list>

14 <https://www.gov.uk/government/publications/notice-to-exporters-202308-russia-sanctions-trade-sanctions-circumvention/note-202308-russia-sanctions-trade-sanctions-circumvention>





**Scenario 7:  
Identifying dual-use  
applications before  
commercialisation**

Lecturer F is a Principal Investigator specialising in **nuclear energy** who has developed an innovative solution for disposing of the radioactive waste produced during the creation of nuclear energy. Lecturer F has been **approached by an overseas company to create a university spin-out** company to market and sell the product.

Lecturer F asked their Head of Department to approve travel expenses for them to visit the overseas company to discuss terms. The Head of Department enquired about the details of the spin-out and recommended that as **nuclear energy falls under the 17 sensitive sectors of the economy** as defined in **the National Security and Investment Act** (NSI Act) that Lecturer F should conduct detailed research into the overseas company. Lecturer F stated that they had confirmed that the collaboration did not require a mandatory notification and therefore did not feel it was necessary to conduct further checks.

The Head of Department **referred the collaboration** to the university's research security team and the technology transfer office (TTO) to **ensure all legal obligations were met**. The research security team identified that Lecturer F's product included multiple components listed on the UK Government consolidated list of strategic military and dual-use items **requiring export authorisation**. The research security team also conducted open-source research on the overseas company and identified news articles citing the **company in disputes over IP theft**.

The research security team escalated the collaboration to the **research risk review board** for their assessment. Given the **dual-use application** of the product and the **concerning reputation** of the overseas company, the university decided to **voluntarily submit a notification** of the collaboration to the UK Government under the NSI Act.

As a result, the Head of Department advised Lecturer F not to travel overseas until the review under the NSI Act had been completed to ensure all legal obligations were met and that Lecturer F's IP was protected.

## Considerations

The absence of a requirement for a mandatory notification under the NSI Act does not mean that a collaboration is low risk. Thorough **due diligence** should still be undertaken, and all **legal obligations must be fulfilled**.

In this situation, if Lecturer F had travelled to visit the overseas company and presented the product without an export license, they would have been in **breach of export control** regulations, therefore committing a criminal offence. As a result, their **reputation** and the reputation of their institution could have been damaged and they could have been **liable to pay a fine or face up to ten years imprisonment**.

The theft of IP can result in a loss of competitive edge, reputational damage, a slowdown in research progress and/or business growth and a loss of trust from partners and funders. Further, the theft of dual-use or sensitive IP can also negatively impact the UK's national security by uplifting overseas military capabilities and/or eroding UK capabilities.

To prevent IP theft, institutions should **identify their most sensitive/valuable IP and protect it** appropriately.

Protective measures include patents, cyber security, non-disclosure agreements (NDAs), selective sharing, clear IP ownership agreements, restricted access (physically and from a network perspective) and policies that set clear specifications for what can be taken overseas.

IP ownership agreements should include:

- identification and notification of arising IP
- protection decisions
- management of IP
- commercialisation and use of IP
- termination agreement
- background and foreground IP
- jurisdiction and governing law
- where information is stored
- allowances and limitations of usage of IP (what, how, when)





## **Disclaimer**

This resource has been prepared by NPSA and NCSC and is intended to aid academic institutions to help them understand and mitigate security risks arising from research, in combination with additional resources and the application of institutions' own judgement. This document is provided on an information basis only, and while NPSA and NCSC have used all reasonable care in producing it, NPSA and NCSC provides no warranty as to its accuracy or completeness.

It is important to emphasise that no security measures are proof against all threats. You remain entirely responsible for the security of your own sites and/or business, and compliance with any applicable law and regulations. You must use your own judgement as to whether and how to implement our recommendations, seeking your own legal/professional advice as required.

To the fullest extent permitted by law, NPSA and NCSC accept no liability whatsoever for any expense, liability, loss, damage, claim or proceedings incurred or arising as a result of any error or omission in the document or arising from any person acting or refraining from acting, relying upon or otherwise using the guidance.

This exclusion applies to all losses and damages whether arising in contract, tort, by statute or otherwise including where it is a result of negligence. NPSA and NCSC separately and expressly exclude any liability for any special, indirect and/or consequential losses, including any loss of or damage to business, market share, reputation, profits or goodwill and/or costs of dealing with regulators and fines from regulators.

Institutions and individuals have a responsibility to ensure that they comply with all relevant legal obligations, as well as any other obligations to which they are beholden. This guidance and the mitigations included in this document should not be considered exhaustive. This guidance raises issues for consideration but does not dictate or purport to dictate what conclusions institutions should reach.



© Crown Copyright 2024

This publication is licensed under the terms of the Open Government Licence v3.0 except where otherwise stated. To view this licence, visit [nationalarchives.gov.uk/doc/open-government-licence/version/3](https://nationalarchives.gov.uk/doc/open-government-licence/version/3)

You may use or reuse this content without prior permission but must adhere to and accept the terms of the Open Government Licence for public sector information.

You must acknowledge NPSA as the source of the content and include a link to the Open Government Licence wherever possible. Authorisation to reproduce a third party's copyright material must be obtained from the copyright holders concerned.

