Advice for working with partners outside the UK – conforming to the 2023 National Security Act and UK government export control.

The 2023 National Security Act and enhanced limitations on acceptable technologies permitted as part of working with a partner external to the UK, have placed additional restrictions on both the University and individuals employed by the University. Working with a person, institution or company external to the UK includes research collaboration, consultancy, equipment access and visitor hosting. This note outlines our obligations in respect of working with partners outside the UK and provides advice on how to ensure compliance with UK legislation so that successful and mutually beneficial collaborations can continue. It is critical that the advice below is considered at an early stage of any potential collaboration or interaction.

1. **UK Government Export Control.**

The UK maintains a list of all items that are subject to strategic export controls. This is known as the consolidated list of strategic military and dual-use items that require export authorisation. The list includes items that are controlled because of international agreements or arrangements as well as further items relating to specific defence or security concerns of the UK.
The two main categories of goods are:

- military goods, software and technology that are specially designed or modified for military use
- dual-use items which are goods, software and technology that can be used for both civilian and military applications

How this affects Universities is detailed at https://www.gov.uk/guidance/export-controls-applying-to-academic-research#overview but, simply, work with colleagues overseas on research projects or other forms of interactions where information is exchanged with colleagues overseas, taking research overseas and exporting technology or know-how require checking against the export control list while considering potential end use and relevant decontrols.

The key decontrols are that information that is already in the public domain and basic scientific research information (i.e. research that has no practical application) is exempt unless there are concerns about the potential use that the information will be used for or concerns regarding the end user (i.e. that they are a military or WMD end user).

In recent years the export control list has become broader and is updated regularly so that it is important to use the latest list and guidance when making decisions. Dependent upon the technical content of a proposed collaboration, the nature of the collaboration and the identity of the overseas collaborator, the University will need to decide whether to approve, perhaps subject to an export licence, ask for modifications to a proposal to limit risk or to reject. The University has detailed guidance on assessing a potential collaboration against export control considerations at https://www.research-operations.admin.cam.ac.uk/policies/export-control. Experience has shown that **it is important to consult this guidance as soon as possible** in a potential collaboration or where there may be potential issues in an existing collaboration. There have been cases where individuals have worked up quite detailed collaboration proposals only to find that the topic is restricted by export control. In other cases the technology focus has shifted during a collaboration requiring a re-assessment against export control. The Export Control Team in the Research Office: researchgovernance@admin.cam.ac.uk are available to provide specific guidance.

The guidance, along with relevant contact points, is there to try and help collaborations to continue successfully; restrictions or rejections of proposals are not in anyone's interest.

2. **The UK National Security Act 2023.**

The National Security Act 2023 is designed to modernise UK espionage laws. A key part of the new legislation is the protection of protected information and 'trade secrets'. The Act applies to a United Kingdom national or an individual who lives in the United Kingdom. This has the potential to affect university researchers in their research, collaboration and commercialisation activities.

New Offences

The Act creates three new offences. The offences only apply when *acting for or on behalf of a foreign power* (or if you *ought reasonably to know that to be the case*) or with the intention to benefit a foreign power.[1] This might include activities funded by a foreign government agency or sending research material to an overseas party who is or is acting on behalf of their government. It also includes any other conduct instigated by, under the direction or control of, carried out with the assistance, of or in collaboration or agreement with a foreign power. As such, this may include collaborative work with an overseas company or university where the partner has close ties with or is under the direction of the foreign power. Particular care should be taken when working with overseas partners whose political system allows significant state control on private enterprises and universities. The offences relate to:

1. **Protected information**: This offence applies to information that has been restricted for the purpose of protecting the safety or interests of the UK or it is reasonable to expect that access to it is restricted.[2] It criminalises obtaining, copying, recording, retaining, disclosing or providing such information where you know or ought reasonably to know it is prejudicial to the safety or interests of the UK. Punishable by life imprisonment or a fine.
2. **Trade secrets**: 'Trade Secrets' are any information, document or other article that are:
    a. Generally not known by experts in the field.
    b. Have actual or potential industrial, economic or commercial value to the UK that would reasonably be expected to be adversely affected if made generally known.
    c. Could reasonably be expected to be subject to measures to prevent it becoming generally known (even if not actually subject to such measures).

    Novel research information could be considered a trade secret if it is subject to measures to prevent it becoming more widely known. The offence applies to obtaining, copying, recording, disclosing, or providing a trade secret when you are not authorised (or know or ought reasonably to know you are not authorised) to do so. Punishable by imprisonment of up to 14 years or a fine.
3. **Assisting a foreign intelligence service**: Any conduct intended to or likely to assist a foreign intelligence service in carrying out UK-related activities (defences exist where the UK is a party in the activity). Punishable by imprisonment for up to 14 years or a fine.

How can I comply?
While the Act does not create new requirements for researchers, it significantly increases the potential consequences of failures to appropriately handle protected information and trade secrets. Researchers should:

1. **Establish whether their work includes 'protected information'.** This is most likely to apply to government information or data, particularly relating to defence or where covered by government security classifications. Such work would normally have specific restrictions forming part of any contract; these should be made clear alongside advice as to how to treat

[1] A 'foreign power' can mean: a) a foreign head of State in their public capacity b) a foreign government or part of government, c) an agency or authority of a foreign government or part of government, d) an authority responsible for administering the affairs of an area within a foreign country or territory, e) a political party that is a governing political party of a foreign government. This includes individuals holding offices in, employed by or exercising the functions of a foreign power.
[2] This includes formally classified information, but also other situations where active restrictions have been placed on the access to information for the purpose of protecting the safety of interests of the UK. It also includes information where it is reasonable to expect that information is restricted (e.g. a sensitive document in a government building).

protected information. If applicable, take advice from departmental computing officers on appropriate data storage and ensure your team is aware of all restrictions.

2. **Ensure they are aware whether any of their work is subject to export controls.** Export controls restrict the release of data overseas, see above, as such controlled data is likely to be interpreted as a trade secret. As such, due diligence according to the University's Export Control Procedures is required before any export.
3. **Be aware of other restrictions** on sharing novel research information including leakage of know-how to external research partners, and projects where researchers recruited to the project agree in advance to restrictions on their freedom to publish (e.g. confidentiality or IP restrictions) and ensure that such information is not shared inappropriately.
4. **Be aware of the foreign power test:** If you are working on a project funded by a foreign government or one of their agencies or if you work with a partner or have a visitor who is or acts on behalf of a foreign government ensure that you and your team are aware of the expectations of the Act (further guidance here). Please note that some universities outside the UK are under the direct control of their government and so may also be subject to the foreign power test.

As with export control, in respect of the National Security Act 2023 there are resources available on-line specifically aimed at UK academic researchers. These can be found at https://heeca.org.uk/index.cfm?action=resources and https://www.npsa.gov.uk/trusted-research-academia.

The University Research Operations Office have an expert team that can be contacted to advise on whether a technology is potentially a restricted technology and thus might require an extra layer of care in communicating information to non-UK partners or colleagues.

Please address any queries regarding export control to the Research Office's Export Control Managers via **researchgovernance@admin.cam.ac.uk** or individually:

- Claire Piffard, Senior Legal Advisor - Claire.Piffard@admin.cam.ac.uk
- Rhys Morgan, Head of Research Policy, Governance and Integrity - Rhys.Morgan@admin.cam.ac.uk
- Nadine Tschacksch, Senior International Research Risk Management Coordinator - Nadine.Tschacksch@admin.cam.ac.uk

The vast majority of external interactions will not be relevant as far as the Act is concerned, but where there is a potential for restricted or protected information to be shared as part of a collaboration or through direct interaction with a colleague, the potential consequences were the restrictions of the Act not adhered to are now considerable and may apply to individuals personally. In this respect, the final responsibility for if and how a collaboration proceeds is down to the individual. The University will do everything it can to ensure that academic freedom to collaborate is retained but it is inevitable that there will be some cases where extra attention to what is shared and with whom will be necessary.

May 24th 2024