Kingston
University
London

Kingston University

Export Control and National Security Policy

Effective from March 2025

Version 1.0

This policy covers compliance with regulations on Export Control, the National Security and Investment Act, and UK Sanctions in relation to research and knowledge exchange activities.

External Compliance Statement

UK Government **export control legislation** restricts the export of information, technology and goods where there is a risk that they could be used for military purposes or other malign purposes. The **National Security & Investment Act (2021)** defined additional sensitive areas of the economy and requires organisations to undertake export control and to inform government about acquisition of certain entities and assets in these areas. The **UK Sanctions list** details organisations and individuals that are subject to sanctions measures that restrict conduct of business transactions. Failing to comply with legislation can carry penalties both for organisations and individuals, which can include criminal prosecutions.

This policy sets out how the university will comply and support its staff to comply as individuals with these regulations in relation to the conduct of research and knowledge exchange (KE) activities. The Provost and Deputy VC, Professor Helen Laville is the senior responsible person for export control and national security matters relating to research and KE, assisted by the Research and Impact team and the Knowledge Exchange and Innovation team in Academic Services. However, it is the responsibility of all staff to be aware of and to comply with the legislation and with the university's written procedures and guidance linked to this policy.

The core of the policy is that each individual must inform themselves regarding the restrictions, and if they intend to send or share anything, material, digital, data or knowledge-based outside of the UK (including to publishers), to ensure (and if in a sensitive area to seek assurance) that it is done in a legally appropriate manner.

1. Introduction

Research and KE at Kingston thrives on wide ranging collaborations with international partners. While the vast majority of international collaborations are welcome and mutually beneficial, it is essential that the university remains alert to activities that may threaten the security and standing of our institution or pose a threat to the UK's national security. Universities and their staff must be aware of how embargoes and restrictions imposed under UK Government legislation for strategic goods and technology impacts on academic activities, including research and knowledge exchange activities, data, methods and information exchange, and ensure compliance with all legal requirements.

How does export control legislation relate to research and knowledge exchange?

Export controls restrict the export and communication of goods and technology designed or modified for military us, where there is a risk, it could be used for military purposes or in Weapons of Mass Destruction or misused for oppression or torture. Controls apply to the academic community as much as any other exporter of goods and technology. Academic research and knowledge exchange collaborations sometimes involve the transfer of physical items and will usually involve technology transfer by electronic or verbal exchange, which also constitute an export. Failure to obtain a licence to export controlled goods or technologies may result in a criminal offense being committed. The legislation is most likely to affect collaborations in STEM subject areas (listed at section 3 of this document), but all researchers must be aware of their legal responsibilities. Export of technology is a frequent activity for most researchers operating collaboratively, and while the majority of transactions fall outside the scope of the controls, the university and individuals must be prepared to make the necessary checks for in advance of any export of sensitive technology.

How does the National Security & Investment Act relate to research and knowledge exchange?

This legislation gives the government powers to scrutinise and intervene in certain acquisitions made by anyone, including universities, that could harm the UK's national security. The Act covers all qualifying transactions involving the transfer of control of entities and assets from one party to another in sensitive areas of the economy. For the university sector this could include the transfer of ownership of spin-out companies or subsidiaries (entities), and transfer of control of intellectual property (assets).

The legislation provides two different notification regimes:

- **Mandatory** – which applies to the acquisition of **Qualifying Entities**
- **Voluntary** – which applies to acquisition of **Qualifying Assets**

NB. Unlike Export Control regulations, for NSIA, transactions within the UK are also in scope.

Qualifying assets and entities are related to sensitive areas of the economy, currently listed as 17 mainly STEM areas listed at section 4 of this document. There is heavy overlap with the high-risk areas identified for export control. Researchers will need to work with their Business Development Manager to initiate checks on whether a business acquisition requires a notification to government under this legislation. For Kingston University, acquisition of entities is a not a frequent occurrence, but transfer and sharing of control of Intellectual Property under consultancy, contract research or research sponsorship arrangements is common. The university and researchers must be prepared to make the necessary checks for transactions in the sensitive technology areas.

How does the UK Sanctions List relate to research and knowledge exchange?

The UK Sanctions list is frequently updated by government in response to world events and can affect all exchanges with specific individuals and specific organisation within countries. Details of overseas external collaborators and customers should be checked against the sanctions list before sharing where Due Diligence checks indicate any grounds to suspect that sanctions may be in force.

2. Scope

People

The policy applies to all staff at or affiliated to Kingston University, visiting academics and to students who engaged in academic research and knowledge exchange. This includes academic staff, researchers, research students, research support staff, research and knowledge exchange managers and professional services staff whose activities may involve the physical export, electronic transfer, or transfer by any means of goods, software or technology subject to export controls. For shorthand, people in scope will be referred to as "researchers" in this document. It's important that all researchers are aware that they are responsible as individuals under the law for their own actions, and that research students similarly carry individual responsibility.

Researchers need to be aware that any research and knowledge exchange related information/ outputs that they send, electronically or physically, or take with them out of the UK constitutes an export. Accessing information while overseas constitutes an export. Sharing information with non-UK citizens while they are in the UK may also be considered an export. It is the individual's responsibility to check if that export is subject to a sanctions embargo or falls in the domain of requiring an export control, through engagement and compliance with the university's due diligence and research management procedures.

Technology types

Most technology controls apply to information that is necessary for the development, production, or use of controlled goods. Some technology controls apply to specific information as described in the lists. This information may take many forms, including but not limited to:

- blueprints
- plans
- diagrams
- models
- formulae
- tables
- engineering designs and specifications
- manuals and instructions, including scientific methods
- data, including preliminary data

3. Export Controls applying to Academic Research and KE

The UK government provides guidance for how the export control legislation applies to academic research which has informed this policy and the university's procedures

An export licence may be required if one of the following apply:

- the software or technology is linked to items in the consolidated list of strategic military and dual-use items that require export authorisation (the control list).
- the researcher has been informed, is aware, or suspects that the recipient of the software or technology intends to use it for WMD (Weapons of Mass Destruction) purposes.

and the answer is yes to any of the following:

- the software or technology is not yet in the public domain (information that is intended to be published and indeed being sent to a publisher is considered not yet in the public domain)
- the technology does not meet the definition of basic scientific research.
- the research is in one of the disciplines that could be targeted by would-be proliferators – see high risk areas listed below.
- recipient intends to use or send the information outside the EU.
- preliminary online searches or other open source checks show the recipient is potentially involved in suspicious activity or has been sanctioned by the UK government

High risk Research and KE

Applied research in certain fields is high risk and could potentially be used/ misused for military purposes. These areas are usually in the science, technology, engineering, and mathematics (STEM) subjects. They include:

- aeronautical and space technology

- applied chemistry, biochemistry and chemical engineering
- applied physics
- biotechnology
- electrical and mechanical engineering
- instrumentation and sensors
- materials technology
- nuclear technologies
- production and process technology
- telecommunications and information technology

Technology transfer: Scope

For goods/technology identified as "controlled", a licence must be in place before the technology transfer overseas takes place.

The tangible transfer of technology can be in many forms. This includes information either written on physical documents or recorded on other media, such as USB flash drives, portable hard drives, laptops, tablets.

Technology can also be transferred in an intangible form by using electronic media, such as email, Teams or social media. The sender has the responsibility to find out where someone is in the world before sending an e-message containing controlled information. The recipient has a duty to consider if an e-message is likely to include restricted information and not access it if outside the UK.

Technology can also be transferred through transmission by audio or video conferencing, and if recordings of presentations are available to overseas audiences.

If a laptop, phone or a memory device with stored controlled technology is taken overseas by any individual, this is a transfer and a licence will be required.

This also applies to visitors from overseas importing or downloading export-controlled material in the UK and subsequently travelling overseas with devices containing the controlled technology. Visitors may need someone else to apply for a licence on their behalf. Sharing technology with a non-UK national is considered a transfer, whether it takes place overseas or in the UK.

Controlled technology uploaded by persons in the UK to a server in the UK, or sent electronically to overseas file storage, and consequently downloaded or accessed overseas by an intended recipient (including UK persons), is a transfer. KU staff should note that storing information on KU provided storage is not considered a transfer, but a transfer will occur if that information is accessed outside the UK by anyone (including person who stored it), or by a non-UK citizen within the UK.

Other countries' export control policies

Other countries also have similar policies. Researchers should check their law before exporting or carrying any information which may be considered sensitive back to the UK.

Some regimes, notably US and EU pass on responsibilities. If you have received goods or technologies, you must check the terms before considering onward sharing or export.

4. The National Security & Investment Act applying to academic research and knowledge exchange activity

The government provides Guidance on compliance with the National Security & Investment Act which informs this policy and our procedures.

It also provides guidance on which areas of the economy are in scope. Subject to certain criteria, you are legally required to tell the government about acquisitions of certain entities in 17 sensitive areas of the economy (called ‘notifiable acquisitions’).Subject to certain criteria, you are legally required to tell the government about acquisitions of certain entities in 17 sensitive areas of the economy (called ‘notifiable acquisitions’).

The 17 areas of the economy are:

- 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

5. KU’s procedures for assessing risks and supporting compliance

Key staff

All staff involved in research and knowledge exchange activity, Research Development and Research Operations Managers (Research and impact team), KE & Innovation team.

Key resources

Staff space guidance on National Security and Export Control, which includes a link to our online screening tool for projects and activities that may fall in scope of the legislation for export control, the National Security and Investment Act, and Sanctions, from March 2025.

Scope

All proposed research and KE activities (funded or unfunded) that involve an external collaborator or funder.

Researchers must notify the Research and Impact team of any new research activity and the Knowledge Exchange & Innovation team of any new KE activity that involves external collaborators and/or funders.

Before embarking on a piece of research or KE, researchers should use the staff space guidance to support them to evaluate risk around these key questions:

a) Will the activity involve transfer by KU staff/students of any materials, technology or know-how outside of the UK, including accessing by KU staff while overseas and access by non-UK nationals in the UK?

b) Could the content of the overseas exchange fall within the scope of sensitive goods or technologies?
c) Could the receiving organisation merit special attention (e.g. links to non-allied military or to sanctioned entities) – and if so, why the collaboration benefits them?
d) is there a transfer of control transaction in a sensitive technology area?

If there is potential for the answer of any of these questions to be yes, the lead academic for the project/activity should use the university's screening tool to support and record appropriate due diligence before the activity proceeds, and complete arising actions. The tool screens project activities in regard to specific technologies, individuals and organisations involved and end users.

Based on the information supplied, your Research Operations Manager will assist with next steps as necessary

- support to check against the control list on the government's publicly available goods checker.
- seek advice from government where a decision is not obvious.
- manage the application through the government's process if an application for an export control licence is required.
- Ensure appropriate collaboration agreements are in place.
- Liaise with the Knowledge Exchange and Innovation team for further checks relating to transfer of control.

Outputs screening: The Library's review process for uploading publications to our repository includes identification of potential risk of National Security and Export Control issues.

6. Travel overseas

If you are travelling overseas, you should consider the information you (or a hacker, or malign government spyware) may be able to access and take steps to ensure that you do not transport and cannot access anything that may constitute a banned export. This includes:

- Only taking the minimum equipment required and ensuring it is free of export-banned material.
- Disabling links and potentially removing accesses e.g. removing KU email from your personal phone for the duration
- Where essential to take computing equipment and working in a sensitive area and/or travelling to a regime that regularly infiltrates via wifi provision, consider asking for a clean machine to take for the occasion, which can be wiped upon return.
- You will be asked to include assessment of export control risks in your travel risk assessment.

7. Related policies

When using mobile devices, it is imperative to follow relevant KU policy to ensure safety of cyber assets. This is more pertinent when information contained may relate to NSIA and export control areas of sensitivity. Please ensure you consider the following policies before using or accessing any information offsite. Please also consider safeguarding issues when travelling abroad, as some overseas operators use opportunities to groom researchers for sensitive information. Please also ensure to address the data protection risk when assessing travel risks.

Travelling, Working abroad and Field Trip policy

IT Security policy