



UNIVERSITY OF  
LEICESTER

# **EXPORT CONTROL POLICY**



**Document Control**

Prepared by	Export Control Policy Task and Finish Group Simon Gill (Chair) Shaun Monkman (Ethics and Integrity Manager – Secretariat) Export Control Policy Task and Finish Group Members
Approved by	Senate
Date of issue	04 September 2024
Version	1
Next review date	04 September 2026



**Policy development steps**

<u>Action</u>	<u>Description of steps taken</u>
Legal implications of this Policy area	<p>By way of export control legislation, the Government places restrictions on the export of goods, technology, software or ‘know how’ to foreign countries, particularly where there is a risk that the export could contribute to the proliferation of weapons of mass destruction (WMD), or be used in terrorism. Sanctions are imposed for other reasons such as to pressure change in the behaviour of regimes or individuals. It is a criminal offence to export goods, technology, software or ‘know how’ without considering the risk of threat to national and international security and obtaining appropriate licences in the event the export is permissible.</p> <p>This Policy has regard to the following legislation:</p> <ul style="list-style-type: none"> <li>- Export Control Act (2002)</li> <li>- National Security and Investment (NSI) Act (2021)</li> </ul>
Consultation for this Policy	<p>This Policy has been reviewed by and received input from:</p> <ul style="list-style-type: none"> <li>• Research Governance Office</li> <li>• Research and Enterprise Division</li> <li>• Colleagues from schools and colleges</li> <li>• Research Integrity Working Group</li> <li>• Financial Services</li> <li>• Legal Services</li> <li>• IT Services</li> <li>• Health and Safety Services</li> <li>• Research and Enterprise Committee</li> </ul>

**Version History**

0.1 DRAFT	First DRAFT document
0.2 DRAFT	Chairs Comments
0.3 DRAFT	Task and Finish Groups Comments
0.4 DRAFT	Wider Consultation Comments
0.5 DRAFT	Post external review by Freeth’s LLP
0.6 DRAFT	Post internal review – to be sent to T&F Group
0.7 DRAFT	Sent to Research and Enterprise Committee
1	Final – Approved by Senate



**Related procedures/guidance:**

- [TR-SOP-2 - Procedure for Obtaining and Registering Export Control Licences at the University of Leicester](#)
- [TR-SOP-3 - Procedure for Managing NSI Act notifications at the University of Leicester](#)
- [Guidance Webpage – Export Controls at the University of Leicester](#)
- [Guidance Webpage – Export Controls – How to apply](#)

**Policy Text**

**1. Introduction**

- 1.1. It is important that all staff are aware of the fact that [governments place restrictions on the export of goods, technology, software or 'know how'](#) to other countries if they could be misused to fuel conflict, threaten national security, support terrorism and crime, violate human rights or proliferate WMD (such as nuclear, chemical and biological weapons, and missiles capable of delivering them). This Policy is applicable to all staff and students as outlined in section 2 below.
- 1.2. Export controls include economic sanctions designed to constrain the activities of target governments, organisations and/or individuals, which pressure them to change their behaviour.
- 1.3. Controls are brought into legal jurisdiction by UK and EU Law which remain post-Brexit.
- 1.4. The National Security and Investment Act 2022 allows the UK government to scrutinise and intervene in certain acquisitions made by anyone, including businesses and investors, that could harm the UK's national security.
- 1.5. This Policy aims to set out the University's position on compliance with export controls and sanctions, in the UK and abroad.

**2. Scope and background**

2.1. This Policy applies to:

- all University staff including full time, part time or agency staff in any of the University's job families, including Honorary Staff and Emeritus Professors;
- staff visiting from other institutions undertaking or supervising activity at, or for, the University; and
- undergraduate and postgraduate students, (both taught and research), whether registered at the University or on temporary placement.

2.2. It should be noted that those based overseas, those travelling to overseas locations, or transferring controlled technology will need to abide by local laws and regulations regarding export controls covered by this Policy. It is the responsibility of the individual to ensure that they familiarise themselves with local rules prior to travelling or, if locally based, prior to starting research or education activity.

**3. Legal Implications**

- 3.1. Failure to comply with the [Export Controls Act 2008](#) is punishable by unlimited fines and up to 10 years imprisonment. It is also a University disciplinary offence.



- 3.2. Failure to comply with the National Security and Investment Act 2022 can lead to various penalties, including financial and criminal sanctions.

#### 4. Monitoring and review

- 4.1. Although Export Controls may be applicable to teaching, in the main they will relate to research projects and enterprise collaborations, therefore the Research and Enterprise Committee will oversee light-touch reviews of this Policy annually to include minor revisions and updating of references. Where the need for more detailed revisions to all or part of the Policy is identified, for example to reflect changes to legislation or changes to funder regulations, the Research and Enterprise Committee will be responsible for revising the Policy and requesting approval from Senate.
- 4.2. The Trusted Research Officer will produce an annual report of all Export Control Licences and all notifications made under the NSI Act. This will be sent to the Research and Enterprise Committee for information, oversight and onward communication as appropriate. Copies of export licenses will be retained by the Trusted Research Officer and overseen by the Research and Enterprise Division.

#### 5. Duties and Responsibilities

- 5.1. It is the duty of all individuals within the scope of this Policy to assist the University in adhering to legislation regarding export controls, no matter the country of origin or operation. Those outlined in section 2 above should follow the relevant processes to ensure that the Trusted Research Team are informed of the need for diligence checks support obtaining export control licences as required.
- 5.2. It is the duty of all individuals within the scope of this Policy to assist the University in adhering to legislation regarding national security.
- 5.3. Postgraduate supervisors must ensure they understand their role and ensure they provide suitable support to those who carry out any relevant research, teaching or acquisition activities.
- 5.4. Senior staff, including, but not limited to Principal Investigators, Doctoral and Dissertation Supervisors and Heads of College/Schools, have responsibility for ensuring that all research, teaching, or acquisition activity undertaken by anyone under the University's auspices has read and understood this Policy before any exports or acquisitions are undertaken.
- 5.5. All individuals within the scope of this Policy must adhere to the principles outlined and the University processes detailed on the University's website.
- 5.6. The Research and Enterprise Committee has a duty to ensure that this Policy and any supporting processes are kept up to date and adhered to as required.

#### 6. Export Controls

- 6.1. Export control refers to a set of legal restrictions on the transfer of certain goods, equipment, materials, software and technology (e.g. data, designs, know-how) from one country to a destination or destinations abroad with the aim of preventing conflict, human rights abuse, weapons of mass destruction (WMD) proliferation and terrorism.
- 6.2. Export controls apply to controlled items which are:
  - **Controlled goods:** goods relating to military, 'dual use' and WMD end-use as defined in detail below in section 6.5;



- **Controlled technology:** information required and necessary to develop, produce or use controlled goods (except in the case of nuclear technology which has a wider definition);
  - **Controlled software:** software designed specifically to develop, produce or use controlled goods.
- 6.3. In the UK export controls are managed by the Department for International Trade, which maintains the [UK Strategic Export Control List](#) to list controlled items.
- 6.4. Controls can be on:
- Physical goods, either permanently or temporarily leaving the country of origin controlled by law, including equipment, components, materials, samples, chemicals and biological agents, and of software or technology stored in a physical format;
  - Electronic transfers of controlled software or technology, (by any means, such as email, Blackboard, Microsoft Teams);
  - Hand carrying controlled technology, plans or data out of the country on paper, laptops, phone, pen drives etc.;
  - Transfers within or outside the UK of any item if you have been informed, you know or you suspect that it is intended to be used in a WMD programme. This includes technology transferred to overseas students during a course in the UK;
  - US-controlled items. US restrictions apply to hardware, software and technology that is located in the UK if it is: (a) US-origin; (b) UK-made incorporating more than a certain proportion of US-controlled components; or (c) UK-made directly from US-controlled technology;
  - Sanctions can be imposed where the transfer of any item or other economic resources is to, or for the benefit of, a sanctioned individual or organisation. US sanctions extend in some cases to supplying any US-origin or US-controlled item to sanctions targets in the UK and worldwide. Trade sanctions restrict the supply of certain items, primarily military, to target countries. More details on sanctions are covered in section 7 below.
- 6.5. Areas of University activity in controlled items likely to be affected by export controls involve:
- **All military-related work:** any item is subject to control if it is specially designed or modified for military use, or if it is intended for military use in a country subject to an arms embargo (for further information visit the [Department for Business and Trade website](#)).
  - **'Dual use':** any non-military item that may be used for military purposes such as: nuclear engineering; viruses, pathogens<sup>1</sup>, vaccines; chemicals with toxic properties; high strength materials; high specification electronics, computers and telecommunications; automation; cryptography; optics and sonar; navigation; submersibles; aerospace; and space. The controls apply to certain items in these disciplines that meet technical criteria defined in the [UK Dual-Use Lists](#) and this can include Artificial Intelligence software.
  - **WMD end-use:** any item, of any sort, if you have been informed, you know or you suspect that it is intended to be used for WMD purposes.
  - **Sanctions:** exporting to countries, individuals or groups subject to UK sanctions as covered in section [7] below.
- 6.6. Where the University activity involves items not specifically listed on control lists or exports to a location not subject to sanctions, consideration and due diligence need to be undertaken

---

<sup>1</sup> Special consideration should be given to genetically modified organisms with increased virulence/pathogenicity/toxicity or contains DNA from a hazard group 3 or 4 virus.



to consider where there is an awareness, knowledge or you have been informed that the items may or will be used for WMD or military.

## 7. Sanctions

- 7.1. Sanctions are legal measures put in place to put pressure on individuals, organisations, regimes or countries to change their behaviour or actions.
- 7.2. It is imperative that those in scope of this Policy are aware of any sanctions imposed by the country they are exporting to. The [UK Sanctions List](#) provides a definitive and up to date list of all sanctions imposed by the UK government.
- 7.3. If exporting **from** abroad, those covered by this Policy must check with the country of origin to assure themselves they are not in breach of any sanction.
- 7.4. Some US sanctions also prohibit the supply of all US-origin items (e.g. US-made laboratory equipment and laptops) to US sanctions targets, which include some organisations and their staff operating in the UK and some foreign research institutions, (notably in China), that may seek collaboration with UK universities, including sending staff or students to the UK.

## 8. Exemptions

There are several areas of academic activity that fall outside of export controls. These are:

- 8.1. **Public domain.** Controls do not apply to software or technology that is '*available without restriction upon further dissemination (no account being taken of restrictions arising solely from copyright)*'. The main considerations are:
  - The software or technology must already be available to anyone without restriction e.g. on a website, at an exhibition, a conference open to the public or with an open access licences such as Creative Commons.
  - It is not exempt if access to it is in any way restricted, except if it is available to anyone in return for payment, in which case it is exempt.
  - Research intended to be published is not exempt until after it is published. **Sending unpublished research work overseas e.g. in the course of teaching, research collaboration or for peer review is not exempt.**
  - The act of publication is not itself subject to licensing unless the technology is otherwise restricted e.g. it contains official classified information.
- 8.2. **Basic Scientific Research.** Controls do not apply to technology that is '*experimental or theoretical work undertaken principally to acquire knowledge of the fundamental principles or phenomena or observable facts and not primarily directed towards a specific practical aim or objective*'. The main considerations are:
  - Technology is exempt if it concerns purely experimental or theoretical work, undertaken to solely obtain new knowledge of the fundamental principles of phenomena or observable facts.
  - It is likely to be basic scientific research if the sole intended output is a published article in a peer reviewed scientific journal;
  - Technology Readiness Levels (TRL) 1-3, but TRL 3 is borderline and needs to be considered case-by-case.
  - It is not directed towards a specific short-term practical aim nor addressing a specific technical problem.
  - This exemption does not apply to software.



- 8.3. **Patent Applications.** Except for nuclear dual-use technology, the controls do not apply to the minimum technical information required to support a patent application.
- 8.4. Where the technology is on the UK Strategic Control List and an exemption applies, an export licence will not need to be applied for.
- 8.5. The exemptions listed above do not apply to University activities where there is an awareness, suspicion or if it is known that the end use is for WMD or the activity is subject to sanction controls.

## 9. Teaching

- 9.1. Export control restrictions may apply when offering teaching within the UK and abroad, both through an overseas campus and electronic means. Guidance is provided on our [Sharepoint pages](#) and by the [government here](#).

## 10. Export Licences

- 10.1. Where a licence is required to export the goods, technology or information, there are three principle licences that may be applied for through the government's SPIRE system:
  - **Open General Export Licence (OGEL):** a general licence applying to exports to the European Union. The licence will not apply to exports for military or WMD use.
  - **Standard Individual Export Licence (SIEL):** to be used where there is no OGEL, a licence permitting the export of a specified quantity of specified items to a specified recipient or specified end-user up to a set quantity or value. Will be for a period of two years or until the export has achieved the specified quantity. A temporary SIEL for a shorter periods may be granted to export goods for demonstration, exhibition or repair purposes.
  - **Open Individual Export Licence (OIE):** a longer-term licence, (generally 5 years), to export specific goods to named locations in quantities that are not specified.
- 10.2. Proposed activities that require an export control licence, (or equivalent), must not start until the licence is obtained and registered with the University in line with [TR-SOP-2 - Procedure for Obtaining and Registering Export Control Licences at the University of Leicester](#)
- 10.3. Once an export licence is received, the Trusted Research Officer is responsible for ensuring that the conditions of the licence will be fulfilled, including any record keeping requirements as referred to in section 12 below.
- 10.4. The Trusted Research Officer must be informed immediately if there is an issue or a suspected breach of any licence condition.
- 10.5. Where items requiring a licence are exported without a licence or there is a breach of the licence conditions, disciplinary action will be considered and the relevant authorities notified.

## 11. US export controls

- 11.1. US export controls may apply to goods, technology and know-how received by the University from the US. US export controls are contained within individual frameworks that include the Export Administration Regulations (EAR) and the International Traffic in Arms Regulations (ITAR).





- 11.2. US export controls can restrict disclosure and access to the product or technology by ‘parties of concern’ even if those individuals are working for or with the University on the same project.
- 11.3. The exporter of the item has a duty to provide the specific US export licence conditions that apply to the item.
- 11.4. Any item subject to US export controls shall not be acquired and/or transferred to any party subject to US export controls unless:
- 11.5. the Trusted Research Officer has received full disclosure of the specific US export licence conditions that must be complied with;
- 11.6. the Trusted Research Officer has agreed a plan or process to ensure that all conditions applicable to the item can be met and/or are fully implemented
- 11.7. A record of the specific US export licence conditions will be maintained by the Trusted Research Officer in line with section 12.
- 11.8. If it is suspected or known that a breach of the US export licence conditions has occurred, this must be raised with the Trusted Research Officer without delay.

## 12. Record Keeping

- 12.1. Export licences obtained will be registered with the University in line with [TR-SOP-2 - Procedure for Obtaining and Registering Export Control Licences at the University of Leicester](#)
- 12.2. A record of advice, exports or transfers of controlled items under each export licence must be made by the exporter in accordance with the requirements set out in the licence on the [Export Control Transfer Form](#). The records must be stored for a minimum period of 6 years or any longer period specified in the relevant export licence.

## 13. Audit

- 13.1. Regular internal checks and audits are conducted to ensure that these principles are strictly observed. Checks should be carried out by both the licence holder and the Trusted Research Officer in line with the stipulations set out TR-SOP-6 Export Control Audit.
- 13.2. The University will also be subject to external audits by external organisations where export licences are obtained.
- 13.3. If any issues are identified by an internal or external audit, or where an issue is raised, these shall be investigated promptly, urgent measures taken to prevent any recurrence, disciplinary action considered and the relevant authorities notified.

## 14. National Security and Investment Act

- 14.1. When considering exporting goods or know how, staff must also be aware that there are also rules set down in the National Security and Investment Act (“NSI Act”) regarding qualifying acquisitions that may create a threat to the UK’s national security.
- 14.2. The NSI Act places a mandatory obligation to notify the government or to make a voluntary notification, when undertaking qualifying acquisitions. The government also has the power to call in acquisitions for a period of six months after the Secretary of State becomes aware of the transaction within the five years following completion of the transaction.
- 14.3. NSI rules may be applicable in the following University activities:
  - developing or forming research centres;
  - developing University or research organisation spin-out companies;
  - funding employees or students in university programmes; and



- donating to an academic institution.
- 14.4. The NSI Act applies to **qualifying acquisitions**. **These** are where:
- the acquisition is of a right or interest in, or in relation to, a qualifying entity or qualifying asset;
  - the asset or entity is from, in, or has a connection to the UK; and
  - the level or control acquired over the qualifying entity or asset meets or passes the following specified threshold:
    - shareholding or voting rights are acquired that exceed thresholds of 25%, 50% or 75%;
    - voting rights are acquired that permit the acquirer to pass or block resolutions; governing the affairs of the qualifying entity;
    - the acquirer can materially influence the policy of the qualifying entity; the acquirer can use a qualifying asset or direct or control the use of the qualifying asset.
- 14.5. **Qualifying entities** within higher education may include a university, a trust, a university subsidiary or university spin out company, a research consortium or organisation. It will also cover private companies or corporations that carry out contractual work with higher education institutions or research organisations.
- 14.6. **Qualifying assets** includes land, tangible, moveable property and intellectual property. Within higher education this may include equipment, formulae, algorithms, software, patents, trade secrets, designs, plans, drawings and specifications.
- 14.7. The definitions of entities and assets and those most likely to be implicated when considering a higher education setting are laid out in the government's document: ['National Security and Investment Act: guidance for the higher education and research-intensive sectors'](#).
- 14.8. **Mandatory Notifications**
- Where a qualifying acquisition of a qualifying entity is made within sensitive sectors, there is a legal requirement to make a mandatory notification.
  - The sensitive sectors are defined by the [Department for Business, Energy & Industrial Activity](#).
  - The acquisition of the entity cannot complete before government clearance is received.
  - A failure to make a mandatory notification will render any transaction void and can leave the acquirer subject to fines and criminal penalties.
- 14.9. **Voluntary Notifications**
- A voluntary notification can be made to the government for a qualifying acquisition of a qualifying asset.
  - This can arise in circumstances where the acquisition is close to a sensitive area or it does not meet the threshold for the mandatory notification but may give rise to a national security concern. If there is a risk that the government may call in, (and subsequently block), the acquisition, a voluntary notification can be used to allow the government to review the acquisition before it is completed.
- 14.10. Staff must familiarise themselves with the government guidance and take action as required, consulting with the Trusted Research Officer.
- 14.11. If you think that you may need to make a notification in relation to the NSI Act then you must contact [TrustedResearch@leicester.ac.uk](mailto:TrustedResearch@leicester.ac.uk) for advice before proceeding.



14.12. Notifications will be made by the Trusted Research Officer using the online service, they will manage the notification in line with [TR-SOP-3 - Procedure for Managing NSI Act notifications at the University of Leicester](#)

14.13. A failure to comply with the NSI Act or to make false or misleading representations in a notification is a criminal offence and will lead to disciplinary action being considered.

## 15. Training

15.1. All staff will be made aware of the need to comply with export controls, specific training around Export Controls from Epigeum will be provided via Blackboard for all staff who self-identify as requiring training.

15.2. The Trusted Research Officer will deliver training on the NSI Act.