Sanctions and Export Control Policy

1. Introduction

Sanctions are restrictive measures taken by the UK government to influence foreign governments, entities or individuals to change their behaviour. They prohibit or restrict the transfer of certain items, services and economic resources to designated individuals, entities and countries.

Sanctions are put in place: in the interests of national security or international peace and security; to promote resolution of conflict; for the protection of citizens in conflict zones; to encourage respect for democracy, law and good governance, human rights or compliance with international humanitarian law. They also aim to prevent gross violations of human rights, terrorism, or the spread of weapons of mass destruction.

Trade sanctions impose either a prohibition or a licensing requirement on the sale, supply, transfer, export or import of specified items (including goods, software, technology, related technical assistance, services and financing).

Financial sanctions are used to: coerce designated persons into changing their behaviour; deny them access to resources they need to continue their offending behaviour; signal disapproval; stigmatise; and potentially isolate and protect assets misappropriated from a country until they can be repatriated.

Export control legislation restricts certain types of goods, software and technology (and related assistance) from being transferred overseas. This can include controlled items (e.g. software) held on a laptop which is taken out of the UK, or which is transferred via a Teams meeting. Although the majority of university activities are likely to be exempt from export control laws, some technical and scientific activities are restricted.

Breaching the sanctions and export control regime is a criminal offence and could lead to fines and criminal or civil action against the University or individuals, as well as cause reputational damage to the University.

This Policy details how the University will comply with legislation by requiring effective due diligence and ensures members of staff understand their responsibilities.

2. Scope, Roles and Responsibilities

The duty to comply with UK financial sanctions applies to all individuals and legal entities who are within the UK's territory. The duty also applies to all UK nationals and legal entities established under UK law irrespective of where activities take place.

The University is required by law to comply with the UK sanctions regime irrespective of where activities take place.

Any US citizens and permanent residents employed by the University need to also individually ensure that they are complying with U.S. sanctions.

This policy applies to all staff at the University. It also applies to visiting academics and students who are engaged in academic research and consultancy.

All staff are responsible for reading, understanding, and complying with this policy and for arranging sanctions screening or enhanced due diligence where necessary. Where advised that an export control licence is necessary, the staff and/or other personnel involved must co-operate and assist by providing the information necessary to obtain an export control licence and comply with all conditions imposed by the licensing.

Staff are independently responsible for ensuring sanctions are not breached with respect to their teaching, research collaborations, and sharing of materials. If a sanction is breached, liability will be shared by both the teacher or researcher and the institution. Principal investigators in research can also be held personally liable.

Staff responsible for postgraduate teaching materials in STEM disciplines must ensure that all materials sent to students overseas comply with export controls by reviewing whether:

any teaching or research content is controlled; anyone granted access to controlled content is working from outside the UK; and if it is absolutely necessary to include controlled content in the materials for remote teaching. (If not, then this should be removed, or an application for an export control licence must be made).

Managers operating in the relevant areas identified in section 9 must ensure that screening is carried out and additional due diligence assessment checks are carried out in high risk areas.

Directors of Research in Schools and Principal Investigators are responsible for ensuring that they and any staff involved with relevant research projects, read and comply with this policy by completing the required due diligence checks and also complying with all licensing requirements relevant to the project if a licence is obtained. All School Directors of Research and Innovation and academics working in high risk subjects (Computing; Engineering, Mathematics and Physics; Natural Sciences (Biosciences and Chemistry)) must undertake mandatory HEECA training to support the ongoing management of risk.

Heads of Schools are responsible for ensuring that staff in their school are aware of this policy and that relevant staff who might be exporting sensitive information via research, international travel or remotely accessed teaching activities have attended relevant training and completed the due diligence checks required. They must also complete mandatory HEECA training and ensure local monitoring of and compliance with any applicable export control licencing conditions.

The Research and Innovation Support Directorate is responsible for: supporting researchers to comply with this policy, including operationally through applications for appropriate licences and/or national security notifications; raising the profile of Trusted Research; and liaising with the Research Collaboration and Advisory Team (RCAT).

Academic Operations team is responsible for supporting and submitting licence applications in non-research areas (e.g. teaching and conferences).

The Governance and Assurance Directorate are responsible (subject to resource allocation) for providing advice and support on how to comply with the legislation, licensing, reporting and record keeping requirements.

Executive Group are responsible for: implementing this policy; monitoring compliance; ensuring effective training for staff; and ensuring that the policy is regularly reviewed and updated as appropriate.

Committee oversight and governance of export control licence activity is assigned to the Research and Innovation Board research activities and to the Academic Strategy, Planning and Performance Board for teaching and other activities.

Audit Committee has overall responsibility for this Policy and for fostering a culture of compliance within the University in relation to the sanctions and export controls regimes.

3.Policy objective

The University is committed to the highest standards of integrity and to ensuring adherence to the law and to its obligations under its banking and insurance arrangements.

This Policy is a conduct risk control measure which ensures that the University and its staff and students remain in full compliance with all export controls and sanctions regulations as are applicable to the University's activities.

4. Policy principles

4.1 The University must comply with the UK sanctions and export control regimes as required by UK law. Any proposed activity that is prohibited by sanctions and would constitute a criminal offence must not proceed.

4.2 The University must comply with the requirements imposed on it by its bank which require the University to ensure that it is also not in breach of US[1] or EU sanctions regimes as well as the UK sanctions regime.

4.3 Sanctions must therefore be considered both for legal and commercial reasons to ensure that activities prohibited by sanctions do not proceed (unless allowed by specific permissions or licences obtained from the UK Government).

4.4 Potential sanctions and export control must be considered **before** an agreement or contract has been agreed in principle or in writing and well before payment or receipt of funds from/to a sanctioned country, entity or person.

4.5 Insurance coverage arrangements must also be considered in respect of all relevant proposed activities. Insurance coverage exclusion is likely to apply to any activity for which the provision of insurance coverage would expose the insurers to any financial or trade sanctions imposed by the United Nations or any government, judicial body, or regulatory agency. This may have wider implications if funding is subject to insurance being in place.

4.6 Due to concerns related to potential for indirect sanctions breach the University's professional indemnity insurers have clarified that the coverage exclusion applies to activities related in any way to Belarus and Russia, but also to any territory within Ukraine that is under the control, or claimed to be under the control, of Russia, Belarus, the People's Republic of Luhansk or the People's Republic of Donetsk.

[1] Save for UK nationals or UK incorporated organisations in respect of some US sanctions on Cuba and Iran as the UK government has retained EU laws blocking the extraterritorial effects of specific US sanctions and protecting UK persons from the effect of the US regime.

4.7 Due diligence must include screening checks on all relevant sanctions and export control lists as identified in section 9 and in Annexes A – D to establish whether individuals or entities are subject to sanctions or if activities are subject to export control legislation.

4.8 Enhanced due diligence must be carried out in relation to high risk activities as identified in section 9 and Annex A. In relation to sanctions this will generally be activities related to sanctioned regimes. This should include the relevant guidance in relation to the particular country as certain regimes have 'blanket conditions' that apply even if there is not a sanctioned individual or organisation involved in the activities. In relation to export control this will be where activities potentially involve controlled exports.

4.9 Director level approval must be obtained in advance of any activity where the outcome of enhanced due diligence has indicated an activity is still high risk due to the nature of the activity and the nature of the sanctions (i.e. there is a clear correlation) or when applying for a licence for permission from HM Treasury's Office of Financial Sanctions Implementation (**OFSI**) for transactions that would ordinarily be prohibited. For example, in very limited circumstances funds may be provided to designated persons e.g. to meet their basic needs. Activity is not necessarily permitted just because it is for a charitable or humanitarian purpose and applications cannot be made retrospectively.

4.10 The University must obtain a licence (subject to certain exemptions) for conducting any of the following 5 activities:

1. releasing information or equipment that is protectively marked 'Official – Sensitive' to any foreign entity overseas or when demonstrating it to them in the UK;
2. taking or sending a controlled item outside the UK, i.e. exporting it;
3. technical assistance, e.g. repair, development, maintenance, training or consultancy;
4. arranging transit through or transhipment in the UK of controlled items, with a view to their re-exportation, i.e. trafficking and brokering;
5. arranging the transit through or transhipment in the UK of controlled items, with a view to their re-exportation i.e. transit and transhipment.

4.11 The University must not sell, supply, transfer, export or import strategic or controlled items which are subject to sanctions and/or embargo regimes without a specific licence. The import or export of some goods is also banned outright. Any activity that is subject to export controls shall not be acquired from or transferred to any person or organisation subject to export controls unless a general licence is available or a specific licence obtained and all conditions applicable to the item are met and fully implemented.

4.12 The University will ensure that all staff, visiting academics and postgraduate research students engaged in relevant disciplines are made aware of how the regulations may apply to their activities, through the provision of information, guidance, support, advice and training.

4.13 All staff must be aware that sanctions imposed by other governments may impact on the University's ability to operate within those jurisdictions and seek further advice from the Assurance team or Legal Services if staff believe that sanctions or export controls may apply to their work.

4.14 The University will comply with reporting obligations, including reporting dealings with designated persons, declaring potential breaches and any offences committed under sanctions legislation as early as possible.

5. Legislative framework and penalties

The UK implements United Nations (UN) financial sanctions that are required to be implemented by member states through Resolutions passed by the UN Security Council. The UK also imposes its own sanctions regime, primarily through:

- the Sanctions and Anti-Money-Laundering Act 2018 (SAMLA) which includes powers for the UK Government to make regulations imposing new sanctions. These may specify:
    - the type of sanction (financial, trade and travel);
    - designated persons who are subject to sanctions;
    - exceptions and licensing arrangements; and
    - amendments, revocations and enforcement measures.

UK sanctions measures are organised into different sanctions regimes each addressing a territory or issue.

In the light of the 2022 Ukraine crisis, amendments were made by the Economic Crime (Transparency and Enforcement) Act 2022 which:

- streamline the process for making sanctions regulations;
- strengthen powers to impose monetary penalties for sanctions breaches; and
- enable reports to be published publicising sanctions breaches even where no monetary penalty has been imposed.

Other relevant legislation under which sanctions or other control measures can be imposed:

- Immigration Act 1971;
- Export Control Act 2002;
- Anti-Terrorism, Crime and Security Act 2001 (ATCSA 2001);
- Counter Terrorism Act 2008 (CTA 2008).

Penalties for breach of sanctions or export controls include various criminal offences for breaching the regulations which are punishable by a fine, imprisonment for up to 10 years, or both. It is also a criminal offence to fail to comply with the terms of any export licence.

Individuals and bodies who breach export controls imposed in other jurisdictions could also be subject to extradition requests.

Related regimes

National Security and Investment Act 2021 allows the government to scrutinise and intervene in certain acquisitions made by anyone, including academic institutions. HE providers are required to consider the need to notify the government before transferring control of a qualifying entity or asset (e.g. by licensing intellectual property) that relates to any of 17 sensitive sectors of the UK economy (which include advanced materials, robotics, AI, quantum technologies, data infrastructure, satellite and space technologies, synthetic biology and transport).

Academic Technology Approval Scheme (ATAS) which requires nationals of all countries (save 38 which are deemed friendly to the UK) to obtain a certificate at the time of their UK visa application if they wish to accept an offer to study one of a number of applied STEM courses at masters or PhD level or to work under University sponsorship in a specific scientific and research-based role. Applicants are advised of the need to obtain an ATAS certificate at the time of application. A certificate must be obtained prior to studying on a listed course or working under sponsorship. The nationality of the intended recipient is not a factor as to whether or not export controls apply. The transfer to a non-UK national, that takes place solely in the UK, is not deemed to be an export. As referenced above, nationality is a factor with other government approvals, such as for ATAS certification which is a requirement for some non-UK nationals to be able to study specific subjects in the UK.

Even if students have ATAS clearance, export controls may apply if they attend lectures, seminars, supervisions or access controlled technology remotely from abroad. Those staff responsible for postgraduate teaching materials in STEM disciplines should undertake due diligence to ensure that all materials sent to students overseas comply with export controls by reviewing whether:

- any teaching or research content is controlled
- anyone granted access is working from outside the UK
- it is necessary to include controlled content in the materials for remote teaching. If not, then this should be removed, or an application for an export control licence must be made.

6. What are sanctions?

Sanctions are measures which impose restrictions on individuals, entities and organisations.

Financial Sanctions: The most common types of Financial Sanctions currently in use are:

- **Targeted asset freezes** – these prevent named individuals and entities from accessing funds or economic resources or from moving money or assets from beyond their own jurisdictions. All those subject to an asset freeze in the UK are listed on OFSI's consolidated list. Where there is an asset freeze, it is generally prohibited to:
    - deal with the frozen funds held or controlled by the designated person (this includes funds exchanged for goods or services);
    - make funds available, directly or indirectly to the designated person;
    - engage in actions that circumvent the financial sanctions prohibitions.

Where there is reasonable cause to suspect possession of funds or economic resources (includes property, vehicles) of a designated person they must be:

- frozen;
- not dealt with or made available to the designated person unless there is a legal exception or OFSI have granted a licence;
- reported to OFSI.

- **Restrictions on financial markets and services** – these can apply to individuals, entities, groups or entire sectors. These have taken the form of investment bans; restrictions on access to capital markets; directions to cease banking or all business relationships; requirements to notify or seek authorisation prior to certain payments being made or received or restrictions on the provision of advisory or other financial services (which includes processing payments).

Banned under the Terrorism Act 2000 – An organisation may be proscribed ('banned') under the Terrorism Act 2000 if the Home Secretary believes it is involved in terrorism and it is proportionate to do so.

Trade Sanctions and controls prevent the export, import, movement, availability or acquisition of goods or technology or objects of cultural interest. Targets may include military and dual-use goods and technology for energy or critical industries, luxury goods and precious metals. They can also prevent land from being acquired, services being provided or procured (such as technical assistance, financial and insurance services). 'Trade' is therefore widely defined and includes functions such as teaching post-graduates, engaging in research collaborations, and licensing intellectual property. Trade sanctions tend to be targeted at a large, unnamed cohort of individuals or entities associated in some

way with a target jurisdiction. For example, 'restricted technology' cannot be transferred to 'a person connected with Russia'.

Trade sanctions are particularly relevant to higher education providers authorised by the Financial Conduct Authority (FCA) to provide financial services. The University has authorisation from the FCA in relation to regulated (consumer) credit agreements.

In limited circumstances, licences may be granted by the Export Control Joint Unit (ECJU), part of the Department of International Trade (DIT) to permit something which would otherwise be prohibited, such as the supply of military technology if it is intended solely for humanitarian use.

Some sanctions (such as import and export prohibitions) are imposed on a geographic basis and may apply to a particular country or territory.

Some sanctions are imposed on a thematic basis relating to a particular issue or cause, such as the Global Human Rights Sanctions Regulations 2020 known as the 'Magnitsky' legislation which sanction individuals for human rights breaches, or the Global Anti-Corruption Sanctions Regulations 2021 which enable asset freezes and travel bans on individuals involved in serious corruption.

Trade sanctions are particularly relevant to research and teaching in applied STEM subjects at masters' level and above. It should be noted that the scope of trade sanctions overlaps with export control and national security controls, but they are not identical. For example, the scope of quantum technologies governed by Russian Sanctions and the National Security and Investment Act 2021 is broader than export controls. If an anticipated export of technology is controlled by both export controls and trade sanctions, it cannot proceed unless relief from both sets of rules has been obtained.

Export control applies to control items which are: goods specifically listed on the UK Strategic Export Control Lists; items specifically designed or modified for military use and their components; dual-use items that can be used for civil or military purposes; associated technology and software; goods that might be used for torture; and radioactive sources.

US Export control legislation

US Export Controls may also apply to goods, technology and know-how which came to the University from the UK and US trade sanctions may apply to US persons who work for or who are based at the University. US export controls are found within 3 legal frameworks: the Export Administration Regulations (EAR), the International Traffic in Arms Regulations (ITAR) and the Department of the Treasury's Office of Foreign Asset Controls (OFAC).

US export controls act to restrict disclosures to 'parties of concern' that apply to controlled products or technology, potentially including disclosures within the UK and even if only a percentage (usually 25% or more) has come from the US. Exporters should notify importers

(such as the University recipient) of any specific licence conditions. Parties of concern appear as a security entity on the US Bureau of Industry and Security list. Additional due diligence is required if a person to whom technology is to be disclosed appears on the list.

7.Definitions

Dealing with economic resources - exchanging economic resources for funds, goods or services, or using economic resources in exchange for funds, goods or services (whether by pledging them as security or otherwise).

Dealing with funds – using, altering, moving, transferring or allowing access to funds; dealing with funds in any other way that would result in any change in volume, amount, location, ownership, possession, character or destination, or make any other change, including portfolio management, that would enable use of the funds.

Designated Person ('DP') – all individuals or entities who are subject to sanctions on the UK Government's 'consolidated list'. (Sanctions also apply to any entity owned or controlled by the DP, such as where a DP holds (directly or indirectly) more than 50% of the shares or voting rights, or the power to remove a majority of the board of directors of a company or where a DP has the ability to direct another entity such as controlling or using another person's bank account).

Economic Resources – assets of every kind, which are not funds but can be used to obtain funds, goods or services (including, but not limited to vehicles, stones, antiques and property).

Excluded Person – individuals designated under the Immigration Act who are subject to a travel ban forbidding them from entering the UK.

Financial products – means money market instruments (including cheques, bills and certificates of deposit), foreign exchange, derivative products (including futures and options) exchange rate and interest rate instruments, transferable securities and other negotiable instruments and financial assets.

Financial services – any service of a financial nature, including processing payments.

Funds – financial assets and benefits of every kind (including cash, cheques, money orders, deposits, balances on accounts, debts, bonds, shares, interest, dividends, credit)

Freezing economic resources – preventing economic resources from being dealt with, or exchanged for funds, goods or services, or they are used in exchange for funds, goods for services.

Freezing funds – preventing funds from being dealt with.

8. What activities are relevant?

Universities must comply with sanctions in connection with their in-person teaching, their online teaching, their research collaborations and ventures, when transferring rights to intellectual property, or exporting IP or other technology, when receiving tuition fees and payment for accommodation, fundraising from alumni and benefactors, obtaining external funding for research projects and when undertaking activities on any foreign campuses (where they will also need to comply with any local sanction laws).

The following activities are considered to be **high risk areas for HEIs**:

- recruitment of students including receiving student fees or carrying out transactions from 'designated persons' (DPs) (individuals or entities) or from prohibited/restricted or higher risk countries
- entering into arrangements or agreements with contractors or suppliers who are DPs or from sanctioned countries or regions
- payments made by a third party company or non-family member from a bank account outside the UK, EU or US
- formal and informal collaborations with partners in sanctioned countries/regions or with designated persons who are subject to sanctions
- presentations at conferences by individuals in sanctioned countries
- sponsors who are designated persons or are organisations controlled by designated persons
- travel to sanctioned countries
- sharing research and knowledge in certain identified fields of study
- staff or foreign students carrying sensitive research out of the UK or downloading it from a UK server whilst overseas
- laboratory equipment or materials exchanged with overseas collaborators
- employment of individuals from sanctioned countries in certain identified fields of study or areas that have prohibited sharing of proscribed technical expertise.

If Financial Conduct Authority (FCA) authorised, receiving fees and handling payments when debt counselling or arranging loans.

Relevant high risk disciplines which may be subject to sanctions or import/export controls on related goods:

- items designed for military use and their components,
- dual use items that can be used for civil or military purposes,
- associated technology and software,
- goods that might be used for torture and radioactive sources.

9. Due Diligence

9.1 The University must undertake sanctions and export control due diligence.

9.2 The University is already required under money laundering legislation to ensure that due diligence/'know your customer' screening checks on third parties are conducted before entering into business relationships.

9.3 The University must undertake sanctions and export control lists checks to ensure that individuals and entities (and any individuals listed as owners or controllers of such entities) are not designated persons or subject to other sanctions or restrictions for the following activities in the responsible areas listed in Annex A. The templates at Annexes B and C can be used to record the checks. A basic flowchart outline is included at Annex D.

9.4 The University must assess all aspects of any proposed project or interaction, including payment and supply chains to identify if any proposed partners, persons, contractors or financial institutions appear on the sanctions list or are owned or controlled by listed persons and seek warranties in contracts to address sanctions risk. Annex B can be used for this.

9.5 Enhanced due diligence checks must be undertaken prior to entering into business relationships with entities or individuals based in the countries deemed by UK, US and EU lists to be 'high risk'. Annex C can be used for this.

9.6 Sanctions list screening must use the relevant online lists to determine whether someone is sanctioned as these lists are continually updated. The following search tools can be used:

UK: https://sanctionssearchapp.ofsi.hmtreasury.gov.uk/

EU: https://sanctionsmap.eu/#/main

US: https://sanctionssearch.ofac.treas.gov/

Currently the following countries are deemed to be '**high risk**' across the above sanctions regimes:

Afghanistan, Armenia and Azerbaijan, Belarus, Bosnia & Herzegovina, Burundi, Central African Republic, China and Hong Kong, Cuba, Democratic People's Republic of Korea (North Korea), Democratic Republic of the Congo, Ethiopia, Guinea, Guinea-Bissau, Haiti, Iran, Iraq, Lebanon, Libya, Mali, Moldova, Montenegro, Myanmar, Nicaragua, Russia, Serbia, Somalia, South Sudan, Sudan, Syria, Tunisia, Turkey, Ukraine, Venezuela, Yemen, Zimbabwe.

However, it should be noted that this list constantly changes. Sanctioned countries lists should therefore be checked to ensure this is current:

UK (under 'Geographic'): UK sanctions regimes list

EU (map and list): https://sanctionsmap.eu/#/main

OFAC (US Sanctioned Country list): Sanctions Programs and Country Information

9.7 Additionally, countries designated as **high risk third countries** under the Money Laundering, Terrorist Financing and Transfer of Funds (Information on the Payer) Regulations 2017 (Schedule 3ZA) should also be considered to be high risk:

Albania, Barbados, Burkina Faso, Cambodia, Cayman Islands, Democratic People's Republic of Korea, Gibraltar, Haiti, Iran, Jamaica, Jordan, Mali, Morocco, Myanmar, Nicaragua, Pakistan, Panama, Philippines, Senegal, South Sudan, Syria, Turkey, Uganda, United Arab Emirates, Yemen.

9.8 Where high risk goods, software, technology (and related assistance) are being transferred overseas the following list and tool should be used: DIT's checking tools may be used for this purpose. Case studies are included at Annex D and in the Export Control Guidance at Appendix C.

9.9 any suspected dealings with a target of financial sanctions (or with a third party who is known or suspected of being connected to a target/DP) must be reported to the Assurance or Legal Services teams via riskandcompliance@kent.ac.uk and by completing a breach report form as any held or controlled funds or resources owned by a DP must be reported to OFSI.

10. Further guidance

Detailed guidance and links to consolidated lists can be found on the following web pages:

FCDO: The UK Sanctions List

HM Treasury's Office of Financial Sanction Implementation (OFSI): The consolidated list

OFAC (US Office of Foreign Assets Control): SDN list (US Specially Designated Nationals List) and consolidated list (non-SDN)

EU: Overview of sanctions

DIT export control: Consolidated list of strategic military and dual use items that require export authorisation.

US Export Compliance Resources for Academic Institutions

US Export Administration Regulations (EAR)

NS&I Act: guidance for the higher education and research-intensive sectors

ATAS: Home Office Immigration Rules Appendix ATAS: Academic Technology Approval Scheme (ATAS)

Related University policies and guidance

- Detailed guidance on export controls is available on the Assurance team's Export Control SharePoint page.
- Academic Technology Approval Scheme Guidance on HR's ATAS SharePoint page.
- Details of the ATAS scheme can be found on the University's website in relation to staff and students
- University Academic Technology Approval Scheme (ATAS) Policy.
- Overseas Travel, Work, and Study guidance on HSES's SharePoint page.

Advice and assistance should be sought from professional service departments as follows:

- Assurance or Legal Services if you are exporting or importing goods, or transferring technologies that are subject to prohibitions or licensing requirements, if you believe that the University has any information or reporting obligations or if there are any suspected dealings with a target of financial sanctions (or with a third party who is known or suspected of being connected to a target/DP) via: riskandcompliance@kent.ac.uk

- Insurance where activities (for example grant funded work) require professional indemnity via insurance@kent.ac.uk

- **Research and Innovation Support (Contracts and Assurance) team** can assist you with a licence application related to your research project or contract via riscontracts@kent.ac.uk

- Joint Head of Academic Operations can assist where you need to apply for a licence in relation to non research (i.e. teaching activities) via HeadsofOperations@kent.ac.uk.

11. Monitoring and review

To ensure the University's principles are effective and strictly observed, regular monitoring will take place via at least annual compliance questionnaire for relevant teams to include details of any heightened sanctions risk which will be included in a report to the Executive Group as well as through internal and external audit mechanisms. If any issues are identified, these must be investigated promptly, urgent measures taken to prevent any recurrence, and the relevant authorities notified.

Due diligence records and approvals should be kept for at least 5 years. All local records held in relation to export controls (correspondence with authorities, the licence and expiry date and any other records which are required to be stored by the authorities) must be copied to the Assurance team via riskandcompliance@kent.ac.uk.

By applying for an export licence ECJU have a statutory right to inspect the University's export records to ensure correct use of licences. When using a licence, the terms and conditions of the licence must be complied with, and appropriate records maintained. A breach of export control rules or the terms of a licence may lead to enforcement action and be subject to criminal and civil penalties.

It is a legal requirement to keep a register containing sufficient detail as may be necessary to allow the following information to be identified in relation to each act carried out under the licence:

1. A description of the act.
2. A description of the goods, software or technology to which the act relates.
3. The date of the act or the dates between which the act took place.
4. The quantity of the goods (if any) to which the act relates.
5. The person's name and address.
6. The name and address of any consignee of the goods to which the act relates or any recipient of the software or technology to which the act relates.
7. Insofar as it is known, the name and address of the end-user of the goods, software or technology to which the act relates.
8. If different from the person using the licence, the name and address of the supplier of the goods (if any) to which the act relates.
9. Any further information required by the licence in question[2].

The record must be kept for at least 6 years from the end of the calendar year in which the export took place or longer if required by the licence. ECJU inspect registers and aim to do so within 6 months of the first use of the licence. All registers must be copied to the Assurance team.
The records will be kept on a SharePoint List maintained by the Assurance Team. The List of Exports is accessible via this link:
https://livekentac.sharepoint.com/teams/GOVExportControlLicensingInformationRecords/Lists/List of Exports/AllItems.aspx

[2] Article 29, ECO 2008

The Governance and Assurance Directorate will communicate with sanctions regulators and staff must cooperate with any requests for assistance in relation to sanctions or export control enquiries.

This policy will be reviewed biannually by the Assurance team.

12. Governance arrangements

This policy will be reviewed by the Executive Group and approved by the Audit Committee.

13. Document control

Version	Author	Description of Change	Date	Reviewing / Governing body	Review or Approval date	Next Review date
0.1	AD Assurance	Policy created	09.22	EG reviewed	06.02.23	N/A
0.2	AD Assurance	Amended to include flowchart, due diligence templates and case studies.	03.23			
0.3	Head of Legal	Minor amendments for clarity	05.23	EG reviewed	05.06.23	N/A
0.4	AD Assurance	Typo in 4.11 corrected	06.23	Audit Committee approved with minor amendments noted	13.06.23	13.06.25
1.1	AD Assurance	Updated: Scope (2), Related regimes (5), US Export control legislation (7), Further guidance (10),	01.25	-	-	N/A
1.2	Assurance Coordinator	SharePoint list link added to section 11, RIS contact details added	04.25	-	-	N/A
1.3	-	Formatting	04.25	-	-	N/A
1.4	AD Assurance	Academic Ops contact email added	05.25	EG review	19.05.25	-
2	-	-	06.25	Audit Committee approved	10.06.25	10.06.27

Annex A

Activity	**Impacted teams or group**	**Action required:** Sanctions check (**using Dun & Bradstreet or see - Annex B template**).	**Action required:** Enhanced due diligence -see Annex C template
New students prior to taking payment	Student admissions, records, visa compliance team, international recruitment.	✓	✘
Masters/Postgraduate applied research and teaching in STEM subjects	Lecturers and Researchers in applied STEM subjects	✘	✓ per course or project
Student sponsors for students	Finance income office, credit control	✓	✘
New commercial customers	The team/business agreeing the relationship	✓	✓ high risk countries
New academic partners	QACO, International Partnerships	✓ -Using own due diligence template	✓ high risk countries
New donors and scholarship donations	Engagement and development team leads	✓	✘
Research and innovation bids and awards	Research team – pre award process	✓	✓
Any international research collaboration	Relevant researcher	✓	✓
New suppliers	Finance payments team/procurement	✓	✓ high risk countries
Student and staff travel	Team authorising the travel/travel supplier	✓ high risk countries	✓ high risk countries

Annex B: Sanctions Due Diligence Assessment Template (or alternatively, a Dun and Bradstreet check should be performed)

Name of Division or Directorate:	
Name of Department	
Completed by (include name and job title):	
Date:	
Full name of person or entity being assessed:	
Address of person or entity being assessed:	
Where an entity which has beneficial owners is being checked, please also check against those identified beneficial owners	
Full name of beneficial owner (where applicable):	
Address of beneficial owner (where applicable):	
Project or context summary:	
Supporting documents (if applicable):	
Sanctions screening check outcomes	
UK: https://sanctionssearchapp.ofsi.hmtreasury.gov.uk/	Result: No match/close match/match
Details of close match/match (if applicable):	
EU: https://sanctionsmap.eu/#/main	Result: No match/close match/match
Details of close match/match (if applicable):	
US: https://sanctionssearch.ofac.treas.gov/	Result: No match/close match/match
Details of close match/match (if applicable):	
Confirmation I confirm that the checks performed do/do not reveal any sanctions restrictions relating to this person/entity (delete as applicable)	Signed: Approved:
Where screening checks are a positive match, no payment or receipt of funds can proceed. If funds are already held, please seek further advice (see below) as the University may have to freeze assets and report to OFSI.	

Please retain a copy of this form for your records and send a copy to riskandcompliance@kent.ac.uk for approval. This email may also be used for requests for further information and advice when reporting a match or partial match.

Annex C: Export Control and Trade Sanctions Enhanced Due Diligence Template (Please read the Export Control Guidance first).

Name of Division or Directorate:	
Name of Department:	
Completed by (include name and job title):	
Date:	
Name of Project (where applicable):	
Project filed/area:	
Project or context summary:	
Project sponsor or partner (if any):	
Supporting documents (if applicable):	

Export Controls are designed to restrict export and communication of sensitive technology and strategic goods for national security purposes. **The controls apply to the academic community and may apply to a range of areas of academic exchange which might facilitate technology transfer, either verbally, physically, or electronically.** To safeguard yourself and your work you must comply with government legislation and the rules governing transfer of certain items. Military and dual use items are under the scope of Export Controls. Dual use items are designed for civil purposes but may be used for military purposes. Please assess all aspects of your project. If export controls apply, you may be required to apply for a licence from the Export Control Joint Unit.

Section 1: Is there an export (or are you asking for another person to arrange on your behalf export of) any of the following:	If yes, please provide further details.
Shipping/sending physical materials (including documents) overseas	YES/NO
Taking physical materials (including documents) overseas	YES/NO
Taking electronic files including software, data, or technical information overseas (via laptop, mobile or another portable device	YES/NO
Accessing software, data or technical information stored on a UK based file system from overseas via remote login or VPN etc	YES/NO
Sending email/chat/screenshots containing code, data, or technical information (included encrypted information) to a recipient overseas or who will access overseas	YES/NO
Discuss, describe or present technical information via telephone, video conference such as MS Teams/Skype/Zoom, screensharing to someone in an overseas location	YES/NO
Upload files to a server/cloud repository with restricted access for individuals to access overseas	YES/NO
Section 2: End Use Controls You must not export items or knowledge if you suspect or have been informed that the items might	

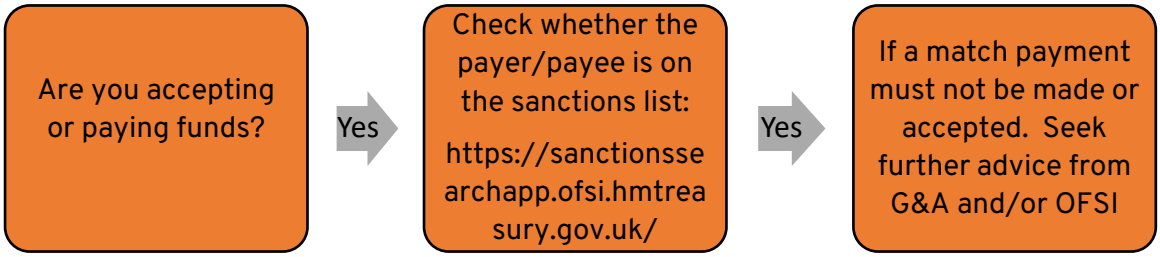
be used to make chemical, biological or nuclear Weapons of Mass Destruction (WMD) or for other military purposes.	
Does the item you wish to export have a **potential** WMD (chemical, nuclear or biological weapons) or military end use or something that is designed for civil purposes, but could be used for miliary purposes (known as dual-use items)	YES/NO/UNSURE (if yes, please provide further details as a licence may be required. If unsure, please seek further advice)
Section 3: Software, Technology and Knowledge	
Will the project involve research into any of the following categories (which apply to STEM subjects but also to some non-STEM research). For example, drones and/or navigation systems. Nuclear, Materials, Electronics, Computers, Telecommunications & Information Security, Sensors & lasers, navigation & avionics, marine, aerospace and propulsion, biotechnology.	YES/NO If yes, state which:
As part of this project, do you expect to be working with technology, equipment, software or samples controlled under UK legislation? To determine this you will need to check: • The consolidated list of strategic military and dual-use items that require export authorisation The government's checker tool	YES POSSIBLY – I have read the guidance and I think my research is controlled, but I am not sure (please seek further advice). NO – I do not work in STEM and my project does not include research into or involve any technology. (If NO, go to **section 4**)
Could the item be described as 'technology or 'knowledge' including written, electronic or recorded information?	YES/NO (If yes, please provide further details)
Is the items software, technology or knowledge that amounts to **basic scientific research** in the public domain? (This means that it must be available without restriction upon further dissemination (other than copyright) and be 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).	YES/NO
Section 4: US imports As part of the project, do you expect to import or use items from the US that are controlled under US legislation? (US legislation is extraterritorial and has to be complied with in the UK. Export documents may state the item is subject to US export control).	YES/NO/UNSURE (If yes, please provide further details and seek further advice).
Section 5: Trade sanctions	Trade sanctions may be particularly wide and include not only transfer of technology,

These include restrictions on activities in certain countries (or which may be received by persons who are ordinarily resident in a particular country) and restrictions on financial dealing with persons or organisations named on government lists.	but also technical assistance in related to restricted goods or technology. Professional and business services (such as audit, IT consultancy and design services) may also be restricted.
Is the destination country/ies in which the person/entity is based **or linked** to a country on the UK/EU/US Sanctioned List? UK sanctions regimes list	YES/NO Name of country (if applicable):
Is the country deemed to be **high risk** under the Money Laundering, Terrorist Financing and Transfer of Funds (Information on the Payer) Regulations 2017 (Schedule 3ZA)	Name of country (if applicable):
EU (map and list): https://sanctionsmap.eu/#/main	Country included YES/NO If yes, please provide further details and a link:
OFAC (US Sanctioned Country list): Sanctions Programs and Country Information	Country included YES/NO If yes, please provide further details and a link:
If yes, is there any correlation between the sanctioned activity and the proposed university activity (for example the sanctioned country may be sanctioned for specific activities which are unrelated to the project or activity).	YES/NO or N/A Please provide supporting comments: If yes, a licence may be required or activity may be prohibited, please seek further advice.
Section 6: Travel and Partners Further information can be obtained by checking the UK Foreign, Commonwealth and Development Office (FCDO) travel information on the relevant country or countries. https://www.gov.uk/foreign-travel-advice (It should be noted that several travel entities are sanctioned for example Aeroflot, Rossiya Airlines, Ural Airlines and Syrian Arab Airlines. **Booking with a sanctioned airline will breach financial sanctions**).	
Is any partner (person/entity) involved on any sanctioned lists? UK: https://sanctionssearchapp.ofsi.hmtreasury.gov.uk/ EU: https://sanctionsmap.eu/#/main US: https://sanctionssearch.ofac.treas.gov/	YES/NO (If Yes, please seek further advice)
Are any controlling persons of other entities involved in the project on the sanctioned lists under sanctions screening?	YES/NO or N/A (If Yes, please seek further advice)
Additional checks carried out:	

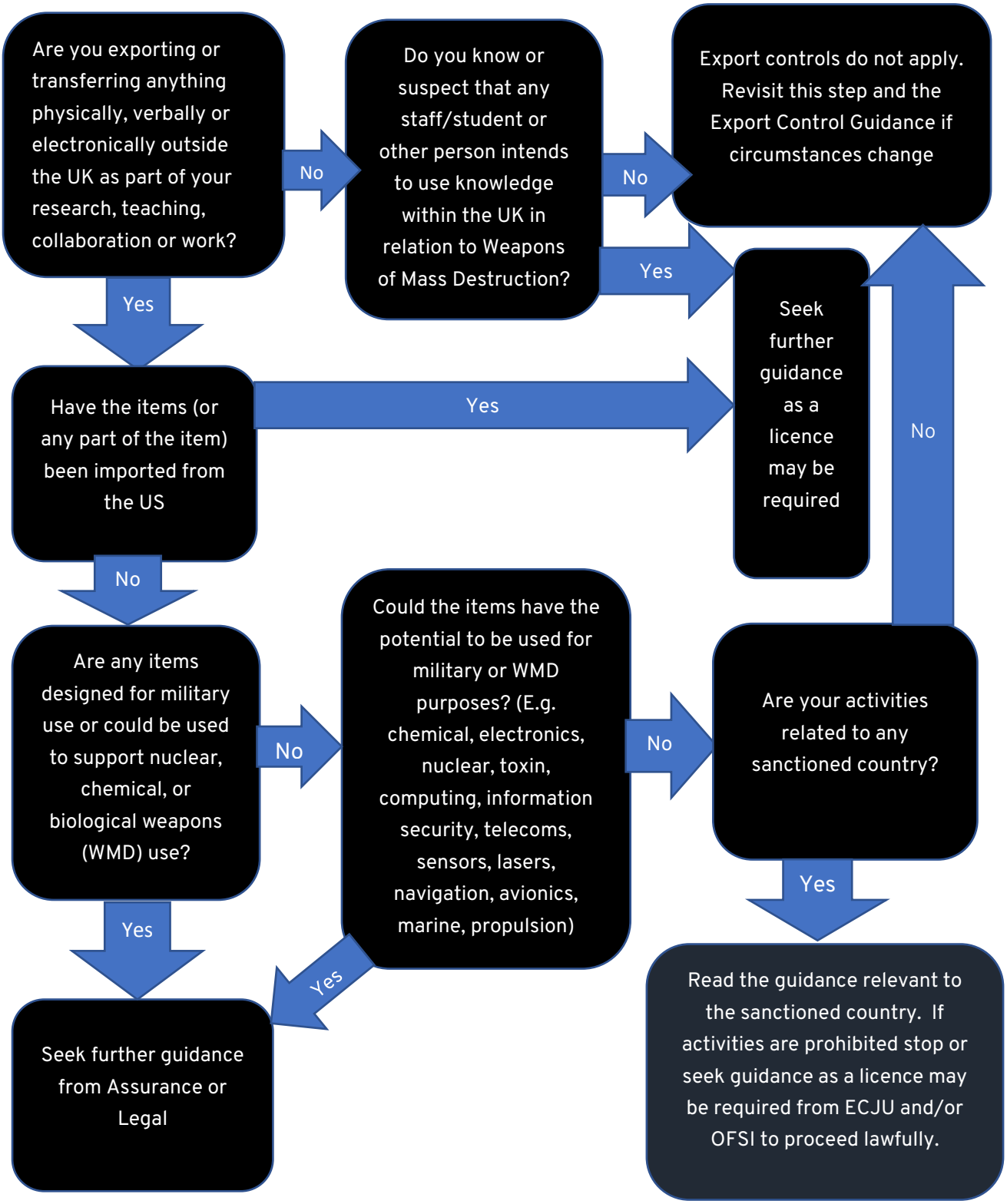
(please insert more rows as needed)	
Further resources:	
Getting the deal through Sanctions 2022 Key information on several sanctions regimes jurisdictions: Australia, the EU, Israel, Japan, Mexico, Russia, South Korea, Switzerland, UK and the US.	

Please retain a copy of this form with your records and send a copy to riskandcompliance@kent.ac.uk
This email may also be used to request further information and advice.

Annex D: Flowchart 1. Financial sanctions due diligence actions flow chart



2.Export control and trade sanctions due diligence actions flow chart. (**Please read the Export Control Guidance for further information**).



Annex E: Case studies (Exporting military or dual-use technology).

Organisation A would like to have outer cases for a military radio manufactured in another country by **Organisation B**. To find out if the latter is able to produce the cases, **Organisation A** must send some drawings of the parts to be made. As the cases are specifically for the military radio, the production drawings constitute technology for the production of a military item. Therefore, a licence is required.

Organisation C manufactures night vision sights for small arms. The products are sold worldwide, and a request has been made for 200 user manuals to be sent to a foreign army. **Organisation C** has made and sold so many of the sights that the user manual can be obtained from their publicly available web site. The foreign army is aware of this but want the manuals posted as hard copies. As a user manual for a military list item, the technology within the manual would constitute technology for the use of a controlled item, so normally an export licence would be required. However, as the user manual is available in the public domain it is released from control by Article 18 of the Export Control Order 2008. That the foreign army has asked for hard copy manuals makes no difference to the freedom to transfer without an export licence, as the public domain exception still applies.

Organisation D makes various controlled mass spectrometers and wants to send some marketing material to a trade fair in another country. The material highlights the typical products supplied and includes testimonials from satisfied customers. Although the company produces controlled items, the publicity material does not include specific information necessary for the development, production or use of the items. The marketing material is therefore not technology as defined and does not require an export licence.

An employee of **Organisation E** sends an email with attachments containing controlled technology to produce military aero-engine components to an overseas partner. The email is automatically routed via a third country. An export licence is only required for transfer to the country of final destination of the email where the intended recipient is located, even where a copy of it is cached (stored temporarily) on a server in the third country.

Organisation F stores cryptographic activation tokens on its servers in the UK that enables cryptographic functions in a variety of information security equipment. Company employees travelling overseas may access these tokens remotely via laptop or another mobile device. A licence would be required for every country from which such access will take place.

Organisation G decides for reasons of cost to locate its data servers in another country. Naval gun designs are uploaded from the UK to those servers. However, access to the designs are restricted so that only employees located in the UK are able to access or download the information. In this case no licence is required because all the intended recipients of the data will be in the UK.

Organisation H makes export controlled CAD software for development of active flight control systems available on its intranet as a service. Access to use the controlled software would not be subject to licensing. However, accessing or downloading the resultant data overseas may be subject to export licences if the data contains controlled technology.

A US employee of **Organisation I** is working temporarily in the UK and remotely downloads UK export-controlled technology, access to which is controlled by the US organisation. No UK export licence is required as in this case the transfer is from the US into the UK. The same US employee then returns to the US with the UK export-controlled technology that he has remotely downloaded and saved on his laptop hard drive. A UK export licence is required for the transfer of controlled technology from the UK to the US. In this example US export controls may also apply as the US employee has accessed US data from the UK.

A UK employee of **Organisation J** transfers controlled technology residing on a server in Iceland to the intended recipient in South Africa. The recipient's server is located in Thailand. An export licence will be required to transfer the controlled technology from the UK to South Africa. The same licensing requirement applies if the exporter or the recipient is unaware of the location of either server.

Organisation J is a cloud service provider. **Organisation K** stores controlled technology on **Organisation J's** servers located in the UK or elsewhere. **Organisation K** has protected the controlled technology stored in the cloud from unintended access, for example by using industry standard encryption, identity and access management or other safeguards. To provide, support and maintain the cloud services, some **Organisation J** technical, administrative and maintenance personnel are located outside the UK. **Organisation K** may require **Organisation J** personnel to manage technical issues in **Organisation K's** cloud environment. No export licence is required because **Organisation J** personnel are not the intended recipients of the controlled technology.

A person in Great Britain uploads dual-use controlled technology to an Icelandic server and responsibility for the controlled technology falls on someone in Northern Ireland. The transfer of technology will be from Great Britain to Northern Ireland. The person in Northern Ireland who is responsible for the controlled technology then grants access to someone in Singapore. Here the export is Northern Ireland to Singapore even though the technology was originally uploaded by a person in Great Britain.

Case studies adapted from Government guidance found here:

https://www.gov.uk/government/publications/exporting-military-or-dual-use-technology-definitions/export-of-technology-remote-access-and-the-use-of-cloud-computing-services

Further academic case studies can be found attached to the Export Control Guidance at Appendix C.