

Edinburgh Napier University Export Control Policy

Introduction/Rationale

Edinburgh Napier University (the University) is committed to delivering excellent research, innovation and knowledge exchange. In pursuit of this mission the University engages in international research collaboration, global movement of researchers and exchange of new ideas. However, some of the knowledge held, goods used, and activities conducted by academics and researchers have the potential to be misused. Some of the work conducted at the University is subject, therefore, to export control law.

Controls over the export of strategic goods or technology have been enacted in the UK and the EU for decades via a consolidated list of controlled military and dual use items (civil technology which may be used for military purposes). In addition, all UN members have been required since 2004 to maintain export controls to prevent the proliferation of weapons of mass destruction. Specific UN or EU sanctions may also apply. As a result, individual academics may need an export licence from the UK Export Control Joint Unit (ECJU) to carry out an activity - failure to obtain one being a criminal offence. Controls cover not only tangible goods, but also software, data, technology and know-how.

The trend towards increased international research collaboration requires researchers and universities to become increasingly vigilant as to when export control law applies. Compliance with export control should also be seen as part of the broader responsibility for research integrity.

This policy is based on the policy and procedures from The University of Cambridge and been adapted with permission.

Scope of Policy

This policy applies to all researchers and support staff employed to conduct research, innovation and knowledge activities under the auspices of the University regardless of how it is funded.

In the academic context, export controls are most likely to apply in relation to scientific and technical research with military, nuclear, chemical, biological, missile and aerospace applications. However, all researchers particularly those in the scientific and engineering disciplines, need to understand export control regulations and ensure that they comply with them.

Researchers should also be aware that United States export control legislation can affect those who import controlled items that were manufactured in the United States.

Policy Aims and Objectives

To ensure that all colleagues understand their responsibilities and the obligations placed on them related to export controls.

To ensure that the University fully complies with the requirements of the export control legislation

Policy Statement

The University is committed to complying with export controls. As such, the University has published this policy and guidance to raise awareness within the institution of export control regulations and set out a procedure for ensuring compliance. It is the responsibility of each individual researcher to ensure that they do not export controlled items without an appropriate licence. Researchers are expected to familiarise themselves with this policy and guidance.

Edinburgh Napier University
Export Control Policy
July 2022

1. What is covered by the Export Control legislation?

'Export' applies to the transfer of controlled goods, technology, software or knowledge from the UK to a destination outside the UK. This includes the physical export of items and also electronic transfer (e.g. fax, email or download). The rules focus on transfer across borders, so taking a laptop overseas when it has controlled items stored on it would be considered export: disclosure to a third person is not necessary. Oral transmission (e.g. conversation, telephone or video conferencing) could be covered where the detail of a technology contained in a document is read out or communicated in a manner that is substantially the same as providing the recipient with the document. The trafficking or brokering of goods between two overseas countries is also covered by the legislation.

Most exports by University employees will be of intangible technology. This might take the form of research data, blueprints, methodologies, plans, diagrams, models, formulae, source code, tables, technical reports, engineering designs and specifications, or manuals and instructions, either written or recorded on other media or devices.

To be controlled, technology must be 'required' for the development production or use of controlled items. This means that it must be responsible for achieving or exceeding the controlled level or function set out in the control lists.

In addition to standard technology exports (i.e. the export of information that is written down in some form), technical assistance can also be controlled. Technical assistance may take forms such as instructions, skills, training, working knowledge and consulting services. Such activities may involve the transfer of controlled intangible technology.

Under exceptional circumstances, transfers within the UK will also be within scope, but only where it is known that the ultimate end use of the item or information is related to WMDs (Weapons of Mass Destruction) outside the UK. These exceptional circumstances will include teaching where the tutor is informed, aware or has reason to suspect that a student intends to use the knowledge provided for WMD purposes.

2. Which items or technologies are controlled?

Items or technologies are controlled in any of the following circumstances:

- a) They are military or dual-use items (i.e. civil items and technologies that could be used for WMD or military purposes) or technology that appear on the [UK Strategic Export Control Lists](#). Technology is only controlled where it is "required" and "necessary" for the development, production, or use of the controlled items.

- b) Items that are not specifically listed on the control lists, but are intended, either in their entirety or in part, for WMD purposes (WMD end use controls). WMD end use controls only apply if you have been informed of, are aware or suspect WMD end use. If WMD end use controls apply, no items, knowledge or assistance of any kind may be given.
- c) Items to be exported to a specific country which is subject to an embargo or sanctions (note that sanctions may include items that are not included on the Export Control Lists).²End use controls apply to sanctioned activities; i.e. an export cannot occur if the exporter knows that the items would be used in relation to a sanctioned activity.
- d) Items that are not specifically listed on the control lists, but you are aware or are informed that the items are (or may be) intended for the incorporation into or for the development, production, use or maintenance of military equipment in a location subject to an [arms embargo](#), or where you are aware that items will be used as parts or components of military goods illegally obtained from the UK.

3. Exemptions

There are exemptions to the controls for software and technology (but not goods). These exemptions will apply to a large amount of the work done at the University. They apply to:

- i. information that is already in the public domain;
- ii. the dissemination of basic scientific research;
- iii. the minimum information necessary for a patent application.

To be in the public domain, information must already be available without restriction upon further dissemination (with the exception of copyright restrictions). Information that has to be purchased from a supplier who controls the supply, requires registration, has restrictions on access, or is subject to Government or Military of Defence security classifications is not considered to be in the public domain.

Basic scientific research is defined in article 18(3) of the Export Control Order 2008 as “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”.

It is important to note that these exemptions do not apply to WMD end use or sanctions controls.

4. US Export Control legislation

United States export controls may also apply to University researchers. US export controls operate via restrictions on disclosure to certain ‘parties of concern’ (see paragraph 5.4 below) that apply to controlled products or technology. This can mean disclosure within the UK and potentially even within a University group. Restrictions apply even if only a percentage of the technology to be disclosed has come from the

US (normally 25%).

The controls operate via specific licence conditions, which exporters are meant to notify importers (i.e. the University recipient). Researchers must be aware if technology has been received under US export licence conditions which restrict giving access to parties of concern. Researchers should seek advice from Research, Innovation and Enterprise to ensure that the exporter provides the specific conditions that must be complied with, which is a duty on the exporter – a general requirement to comply with US export control law should not be accepted.

Parties of concern are:

- entities on the US entity list or
- to nationals of prohibited countries

this is listed at <https://www.bis.doc.gov/index.php/policy-guidance/lists-of-parties-of-concern>.

If a person to whom the technology is to be disclosed appears to be on one of the lists, additional due diligence is required before proceeding, in particular consulting the exporter. Researchers are encouraged to consult with Research, Innovation and Enterprise for assistance. Depending on which list applies there may be a strict export prohibition or lesser limitations and requirements.

University personnel receiving US technology must be mindful at all times of any US export licence limitations and restrictions that apply and seek advice where necessary.

5. Responsibilities

The responsibility for compliance with export control regulations ultimately rests with the individual Principal Investigator (PI) who intends to export goods, technology, software or knowledge outside the UK or use technology imported from the United States of America.

Relevant Departments should ensure that this policy is drawn to the attention of new staff on appointment.

To assist PIs in meeting their obligations, the University has developed the following compliance procedure that all PIs are expected to follow. In general at the time of data management plan review we will assess whether any of the outputs or services used might be in scope of the legislation. In addition, an [export control guide and toolkit](#) is available. A quick guide to the actions required of all researchers to help ensure compliance with export control legislation is provided as Appendix 1 of this policy.

The Head of Research Governance will be the University Export Control Manager (ECM). The Contracts Officer and Project support teams (Research Funding

Managers and Business Development Managers in Research, Innovation and Enterprise will also be provided with training to enable them to support the process and offer advice.

The Head of Research Funding and Services will act as the University's Export Control Director (ECD) and has overall responsibility for this policy and procedures. Contact details for the ECD and ECM are provided on the [University's Export Control website](#).

PIs, particularly in science and engineering disciplines, should ensure that they:

1. are aware whether their research may be subject to export control legislation;
2. have read and understood this policy;
3. consider the [export control guide](#) and [University Export Control website](#), whenever embarking on an activity that could:
 - lead to the physical, electronic or verbal export outside the UK of goods, software or technology:
 - with the potential for military use, dual use or WMD use;
 - that are covered by sanctions or embargo when exported to their intended destination;
 - that they have been informed by the ECJU are covered by export control.
 - a. involve the transfer of knowledge within the UK for use in a WMD programme outside the UK (including through teaching);
 - b. involve the transit of goods, software or technology through the UK.
4. Seek advice from the ECM when they suspect that export controls may apply to their work;

If a PI suspects that an export licence may be required they will be required to complete a licence enquiry form with the assistance of the ECM. The ECM will work with the PI to decide whether a licence should be applied for. This will require significant input from the PI who is likely to be best placed to judge whether their export falls on the control lists.

If a licence is required the ECM will work with the PI to decide whether the export can take place under an existing Open General Export Licence and if not which type of licence is required.

The ECM will work with the PI to prepare the licence application. The application process will require considerable input from the PI and may require a signed undertaking from the end user of the item or technology

Once a draft licence application has been prepared, the ECM will complete a Licence Request Form for approval by the ECD. Upon approval, the ECM will apply for an export licence using the ECJU's licencing system (SPIRE).

Once the licence has been issued, the ECM will discuss any terms of the licence to the PI as well as their record keeping responsibilities (see below). Export cannot take place until the licence has been issued and it must comply with all terms of the licence.

When exporting physical items using a freight forwarding service or similar, it is important to ensure that they satisfy professional standards. It is also essential to provide clear written instructions to the freight forwarding agent which will include the full licence details, an explanation of the implications of licence for the export (e.g. for routing) and their responsibility for documentation (e.g. returning completed customs declaration for records).

6. End-user due diligence

The vast majority of collaborators and end-users will be legitimate. However, it is the responsibility of anyone who exports controlled items to be vigilant for end-users whose intent is to procure or divert items for proscribed purposes (such as proliferation of weapons of mass destruction or military end-uses) or to proscribed destinations (such as those under embargo). For details on sanctions and embargos see the [government's guidance](#).

Should a PI or the ECM have suspicions regarding an end-user they must seek the advice of the ECO.

Examples of behaviour that may be of concern include:

- The end-user has known links to an overseas military;
- The end-user or consignee is reluctant to offer information about the end-use of the items;
- The end-user or consignee is reluctant to provide clear answers to standard questions regarding the export, themselves or their business;
- The claimed end-use is unconvincing given the customer's normal business, or the technical sophistication of the items;
- Routine installation, training or maintenance services are declined;
- Unusual shipping, packaging or labelling arrangements are requested;
- Unusually favourable terms are offered in return for the export;
- The item is planned to be installed in an area to which access is severely restricted or is unusual considering the type of item to be installed;
- There are unusual requirements, such as excessive confidentiality about final destinations, customers, or specifications of items;
- There are requests for excessive spare parts or lack of interest in any spare parts that would normally be provided.

Particular attention should be paid to end users who are new to you and the University and for which your knowledge is incomplete or inconsistent. If you have any concerns seek advice.

7. Record keeping

The ECM will be responsible for ensuring that the following records are maintained:

- Licence Request Form
- Details of the consignee and end user (as well as anyone else involved in the export) including name, address and country
- The nature of the export and description of the item exported (including quantity)
- Original source of the items exported (including supplier details)
- Correspondence with the ECJU relating to the project
- The export licence
- Records (including dates) of each transfer under the licence
- The date of the transfer or the period of time over which the transfer takes place
- In the case of software, the software that is exported and the details of the transfer
- In the case of a transfer by electronic means, the email or facsimile
- Any further records required by the licence or judged relevant by the ECM

These records will be kept for a minimum of 6 years from the end of the year in which the export took place or longer if required by the licence.

A register of all export licences obtained by the University will also be kept by the ECM.

8. Audit

Export licences may be subject to audit by the ECJU's Compliance Unit to ensure that the terms of the licence have been complied with. The ECD, ECM, and the PI involved in the export will be involved in the audit.

The ECJU expects that the ECD will also undertake an annual internal audit of a small number of existing licences (the number will be proportionate to the number of active licences). The results of the audit will be reviewed and any necessary changes to this policy will be made.

An internal audit checklist has been prepared to guide this process, see link below. The checklist and supporting information will be stored by the ECM for a minimum of 6 years following the audit.

9. Guidance and Training

Training on export control is provided by the ECJU. The ECM will be expected to attend at least one such session upon taking up their position and periodically after that to refresh their knowledge.

The ECD will ensure that sufficient training is available for researchers whose work may be subject to export control. The ECD and ECM will work with Departments and Faculties to identify staff who work with controlled items or technology and require training. Records will be kept by the ECM of the training provided to researchers.

This policy and additional guidance will be made available on the Research

Innovation and Enterprise website:

<https://staff.napier.ac.uk/services/research-innovation-office/policies/Pages/Research-policies.aspx>

And [Export Control Guidance \(napier.ac.uk\)](https://www.napier.ac.uk/export-control-guidance)

10. Committee oversight of policy

1. Research activities

- a. Research, Innovation and Enterprise will risk assess via data management review and report any in scope activities to BEIS and Research and Innovation Committee.
- b. Research and Innovation Committee will report to Academic Board via meeting minutes.
- c. Export controls are added to the operational risk register to ensure visibility of corporate risks which will be reviewed by Risk and Resilience Committee.

2. Learning and teaching activities.

- a. Collaborative Provision Committee supported by the Department of Learning and Teaching Enhancement will risk assess and monitor any in scope reportable activities in terms of teaching materials going overseas to BEIS and report any in scope activities to BEIS if required.
- b. Collaborative Provision Committee will report to Academic Board any reports received of any such activity which will be captured in its minutes.

3. Other University activities

- a. Procurement (which covers software purchases) is supported by the University's Procurement team provided by Advanced Procurement for Universities and Colleges (APUC) Ltd, the Procurement centre for expertise for Scotland's Universities and Colleges, whose processes ensure all applicable procurement rules and legal requirements are followed and will report any in scope activities to BEIS if required.
- b. Procurement/finance controls are subject to periodic internal audit which provides assurance on control systems to Audit and Risk Committee and Court.

Appendix 1: Actions to ensure compliance with export control

The following steps should be followed by all researchers to help ensure compliance with export control legislation.

1. **Know your research:** Be aware of the [export control lists](#) and whether your research has the potential to be covered by them.
2. **Know your exports:** If you undertake an activity that could lead to the export of goods, software or technology outside the UK or the transfer of knowledge within the UK for use in a WMD programme outside the UK consult the University [Export Control website](#) and the export control lists. If you believe that export controls may apply, seek advice according to the University's export control policy (above).
3. **Know your collaborator:** Consider new collaborators carefully. Is your collaborator:
 - a. from a sanctioned country on the ECJU published list <https://www.gov.uk/guidance/current-arms-embargoes-and-other-restrictions>
 - b. Any collaborator from another country having or developing a nuclear programme
 - c. On the US entity list OR
 - d. Is the collaborator linked to their national military complex or genuinely only civil?
 - e. Is the only use of the technology is for military purposes (e.g. stealth technology).

If this process raises concerns about the collaborator contact Research, Innovation and Enterprise (RIE) for advice. RIE will likely support you to make an enquiry to the ECJU to establish whether the collaborator is of concern. If they are, any collaboration is likely to require a licence.

4. **Know your technology inputs:** All researchers need to be aware of whether they are using US controlled technology and if so check:
 - a. whether the technology is subject to restrictions on providing access to nationals of a prohibited country (this will apply even if that individual is based in the UK, a University employee, member of the research team, or visiting scientist); and
 - b. whether the exporter is on the US list of [parties of concern](#).
 - c. AND IF a or b apply work with the Research, Innovation and Enterprise to contact the exporter and the relevant US licensing authority for advice (BIS for ITAR and Commerce for EAR control)