QMUL Export Controls Guidance

Using your devices overseas

Version 1.0 (January 2024)

Please follow the National Protective Security Authority 'Trusted Research Countries and Conferences Guidance' which outlines main challenges presented when working or travelling overseas. Please note the guidance below will be updated regularly based on the legislation changes.

All QMUL staff and students must ensure compliance with UK export controls when travelling overseas for international research activities, attending conferences, or carrying out QMUL duties while traveling privately. UK Export Controls apply both to the direct transfer of materials overseas, such as presenting at a conference or discussing with a collaborator, and to indirect transfer, such as accessing personal or institutional (managed and unmanaged) devices and USB sticks overseas.

While not all data/technology/software that researchers work on will fall under export controls, the staff and students need to identify which, if any, do. Export controls apply to military and dual use items/technology (items/technology for civilian use but that have enhanced capabilities that are useful in chemical, biological, radiological, nuclear or conventional weapons), as well as other items if there is a risk that they may be intended or diverted for purposes connected with the development, production or use in military or for WMD, or means of their delivery. For more information on what is controlled, please see UK government export control guidance.

Conferences

Data/technology/software that have been published and are freely available and are already in public domain does not fall under UK export control. However, the intention to publish is not sufficient for this exemption.

If you want to present or discuss any data/technology/software that falls under export controls before they are published, you will need to obtain an export control license before traveling overseas.

Taking your device overseas

All staff and students need to follow the IT Services Policy on traveling to high-risk countries. The National Cyber Security Centre highlights that the regimes that continue to present the most acute cyber threat to the UK and its interests are Russia, China, Iran, and North Korea. For travel to these countries, a "loan PC" will be required regardless of whether your primary device is managed or un-managed and no data should be copied to these laptops.

For travel to countries listed as embargoed destinations under military end use controls, ITS managed or un-managed device will be appropriate, in line with IT Self-Managed Device Policy. However, you need to check if any of the technology/information on your devices falls under UK Strategic export controls list or if you have reasons to suspect information on your device could be used for production, test or as analytical equipment and components, for the development, production or maintenance of military items/technology. If so, an export control license would be required, or you need to remove any such data/technology/software before you travel.

For all other countries ITS managed or un-managed device will be appropriate, in line with IT Self-Managed Device Policy. However, any data/technology/software stored on the device that falls under the UK export controls would have to be removed or an export control license would have to be obtained before travel.

In cases where it would be impractical to remove all the relevant data/information, consider arranging a "loan PC" on which only non-controlled information/data can be taken.

Accessing QMUL servers/cloud data from abroad

Please note that if the data/information/technology falls under the export controls then an export control license will be required to access it when overseas e.g. via SharePoint/Cloud or email. This requirement applies to all countries outside the UK.

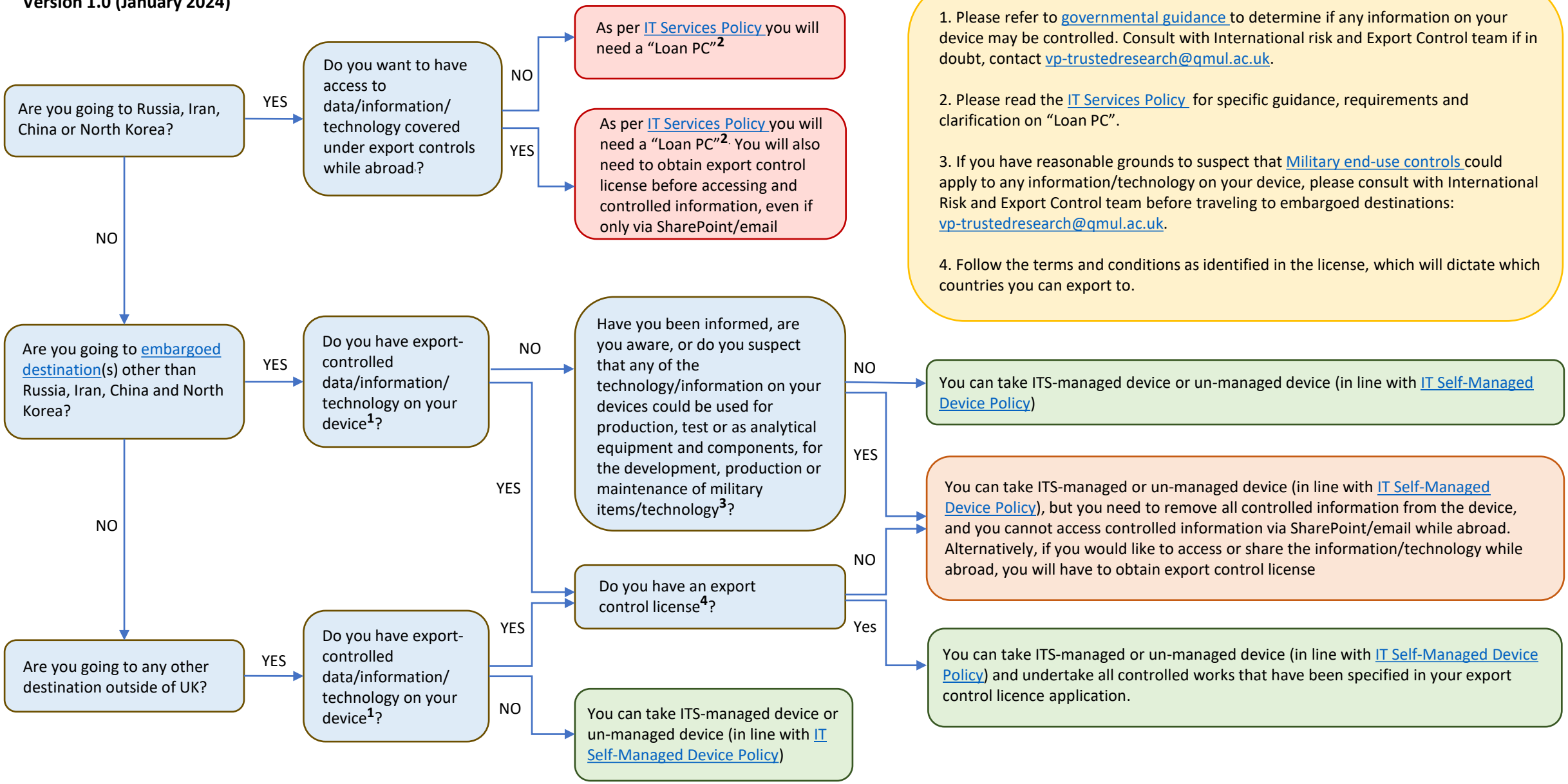
Use Webmail instead of Outlook to access your emails from abroad. If you have an attachment that you suspect contains controlled data/technology/software, do not open it abroad. Do not use the University shared drives or other University servers to access your controlled information from abroad without a license.

Flowchart for implementation

When planning your travel make sure you have checked the Working Off-Site Policy and Guidance and informed the university insurer of your travel. Please refer to the flowchart below to determine the type of device you can take and whether an export control license is required. Remember, if required, obtain an export control license before you travel overseas.

Export controls – using your devices overseas when travelling for QMUL duties or attending conferences

Version 1.0 (January 2024)



1. Please refer to governmental guidance to determine if any information on your device may be controlled. Consult with International risk and Export Control team if in doubt, contact vp-trustedresearch@qmul.ac.uk.

2. Please read the IT Services Policy for specific guidance, requirements and clarification on "Loan PC".

3. If you have reasonable grounds to suspect that Military end-use controls could apply to any information/technology on your device, please consult with International Risk and Export Control team before traveling to embargoed destinations: vp-trustedresearch@qmul.ac.uk.

4. Follow the terms and conditions as identified in the license, which will dictate which countries you can export to.