IT Services Policy

IS14 - Staff Travelling to High-Risk Countries

Prepared by: ITS Services – Information Security
Version: 1.1
IS14 - Staff travelling to high-risk countries

Queen Mary University of London - Open

Last Review Date: September 2023  Next Review Date: September 2024

Reviewers: IT Leadership Team (ITLT), Information Governance Group (IGG)

Policy Owner:
Name/Position: Head of Information Security – Tim Passe

Revision History

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
<th>Author</th>
<th>Date</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.0</td>
<td>Initial Version</td>
<td>Azad Hajiyev</td>
<td>September 2023</td>
</tr>
<tr>
<td>1.1</td>
<td>Updates</td>
<td>Azad Hajiyev / Tim Passe</td>
<td>October 2023</td>
</tr>
</tbody>
</table>

Authorisation:

Name / Position: Rachel Bence, Chief Information Officer

Signature: R. Bence

Date: October 2023
Contents

1 POLICY STATEMENT .............................................................................................................................................................................. 4
2 WHAT IS A HIGH-RISK COUNTRY? ....................................................................................................................................................... 4
3 DOES THIS POLICY APPLY TO ME? ..................................................................................................................................................... 4
4 RISKS WHEN TRAVELLING TO HIGH-RISK COUNTRIES .................................................................................................................. 4
5 GENERAL GUIDELINES FOR TRAVELLING TO HIGH-RISK COUNTRIES ............................................................................................ 5
6 GUIDELINES BY CATEGORY OF TRAVELLER ........................................................................................................................................ 5
7 COMPLIANCE .................................................................................................................................................................................................. 6
8 RELATED DOCUMENTS ............................................................................................................................................................................. 6

APPENDIX: GUIDANCE FOR THE USE OF LOAN LAPTOPS IN HIGHER RISK COUNTRIES .............................................................. 7
LOAN PC AND TRAVELLER POLICY ACCEPTANCE FORM ............................................................................................................................. 14
1 Policy Statement

This policy outlines the risks associated with travelling to high-risk countries, defines different categories of travellers to such countries and the way the risk should be mitigated for each category of traveller.

The Policy aims to:

- Provide clear guidance to University staff and postgraduate researchers on the use of technology in high-risk countries.
- Instructions for end users on how to be vigilant and safely travel to high-risk countries.

2 What is a high-risk country?

A “high-risk” country will be hereby defined, per NCSC guidance, as “state actors, with malign intent, that do not operate under the same legal and democratic framework” as the United Kingdom and other “responsible, democratic” countries. At the time of writing, the NCSC’s list of high-risk countries can be found at https://www.ncsc.gov.uk/collection/annual-review-2022/threats-risks-and-vulnerabilities/state-threats.

At the time of writing, the countries included in the NCSC’s list of high-risk countries are:

- Russia
- China
- Iran
- North Korea

* IT Services endeavours to keep all its guidances up to date, however, please refer to the NCSC site or contact IT Services if you have any concerns about travel to your intended destination.

3 Does this policy apply to me?

There are three main categories of users who fall into the scope of this policy:

- Professional Services Staff permanently based in the UK who visit a high-risk country.
- UK-based Academics & Postgraduate researchers visiting a high-risk country.
- Professional Services staff, Academics and Postgraduate teachers permanently based abroad in a high-risk country.

4 Risks when travelling to high-risk countries

The NCSC advises that the type of cyber security threats that high-risk countries present varies widely, including:

- Cyber-enabled espionage - unauthorised access or transfer of secret, classified or sensitive information to gain advantage over rivals.
- Destructive cyber capabilities - using tools such as wiper malware to damage IT systems or institutions.
- Cyber-enabled theft - to further strategic advantage or domestic control, for example of Intellectual Property or personal data of citizens.
- Hack and leak - stealing and publishing sensitive or restricted information to embarrass states or institutions or to undermine social cohesion.
5 General Guidelines for travelling to high-risk countries

Devices managed by the IT Services department are set up and monitored to help prevent many types of attack, however, they cannot be fully protected. The protections can be bypassed if a malicious actor is able to gain physical access to the device or coerce a legitimate user of the device. To minimise risk to University data and infrastructure:

- Travellers shall not take an ITS-managed device to a high-risk country.
- Travellers should use a “Loan PC”.
  - Loan PCs are purpose-built to minimise risk to QMUL data.
  - No data should be copied to these laptops (hard drive or any other storage media on this laptop). These considerations apply especially to data that must be protected by UK law and to Research Data and Results.
  - QMUL resources shall be accessed online (see Appendix: Guidance for the use of loan laptops in higher risk countries). Desktop applications shall not be installed on these PCs. Detailed instructions can be found in the Appendix: Guidance for the use of loan laptops in higher risk countries.
  - Loan PCs shall be wiped and rebuilt on an annual basis by ITS or the School IT representative.
  - Upon receipt of the Loan PC, the user shall complete a policy acceptance form that will be retained by ITS or the School IT representative.

- Ensure all software on your devices is up to date before you travel.
- Don’t install unnecessary software on your device.
- If a university device is seized, accessed, or modified in any way, the user shall report the incident to the IT Service Desk immediately. The Service Desk is available online at https://its.qmul.ac.uk/ or via email at servicedesk@qmul.ac.uk

In this context “accessed or modified” includes but is not limited to:

- Inserting USB devices that are not trusted by the legitimate user.
- Installing software at the direction of an untrusted party or official.
- Opening the device and making changes to the components inside.

- If a user is forced to disclose a password to a QMUL device or application, the user shall report the incident to the IT Service Desk immediately. The Service Desk is available online at https://its.qmul.ac.uk/ or via email at servicedesk@qmul.ac.uk

6 Guidelines by category of traveller

Professional Services Staff

- A Queen Mary Managed Device will be issued only for work in the United Kingdom or other low-risk countries. This device is not to be taken to any High-Risk Country.
- If a user is to visit any High-Risk Country, they will need to request a Loan PC by logging a Service Desk Ticket giving at least 10 days’ notice
  - ITS has a small number of Loan PCs available for Professional Services Staff for occasional travel. If you require a permanent Travel laptop this will need to be funded by your department.
- Upon receipt of the Loan PC, the user shall complete a policy acceptance form that will be retained by ITS.
- On return to the UK, user shall immediately return the device to ITS who will wipe the device.
- Whilst travelling, if the device is seized, the user shall report the incident to the IT Service Desk immediately. The Service Desk is available online at https://its.qmul.ac.uk/ or via email at servicedesk@qmul.ac.uk
Academics and Postgraduate researchers

- A Queen Mary Managed Device (MSR/MRDS) will be issued for use while in the United Kingdom or low-risk countries. **Managed devices shall not to be taken to any High-Risk Country.**
- Schools shall provide travellers with a laptop for use when visiting a High-Risk Country.
- The Microsoft Office 365 desktop client shall not be installed on unmanaged devices except for MS PowerPoint.
- Upon receipt of the travel laptop, the user shall complete a policy acceptance form that will be retained by the School IT representative.
- If the device is seized, the user shall report the incident to the IT Service Desk immediately. The Service Desk is available online at [https://its.qmul.ac.uk/](https://its.qmul.ac.uk/) or via email at servicedesk@qmul.ac.uk
- Whilst in the UK, the travel device can be used on the Eduroam network.
- Devices used for occasional travel to high-risk countries shall be wiped and the required software reinstalled immediately upon return from each trip, or at least annually. This will be conducted by Faculty IT representatives following processes set out by ITS. Information Security will periodically audit devices used for travelling to high-risk countries to ensure compliance.

7 Compliance

Compliance with the policies and procedures laid down in this document will be monitored via policy acceptance, together with independent reviews by both Internal and External Audit on a periodic basis.

The Assistant Director - Office of the Chief Information Officer, in conjunction with the Head of Information Security, is responsible for the monitoring, revision and updating of this document.

8 Related Documents

ITS Policies [https://www.its.qmul.ac.uk/governance/policies/]
Appendix: Guidance for the use of loan laptops in higher risk countries

Key points

- Use the browser version of applications where possible (section 2). Only use the desktop client version if the browser version does not work for you (section 3).
- Make sure that you log out of all accounts before travelling through customs (section 2.3).
- The Loan PC shall not be used for any purposes upon return to the UK. Users shall arrange to return the ITS Loan PCs to ITS immediately upon return to the UK.

1. **Loan Laptop Account**

To login to your loan laptop, you will have a specific local account for that laptop, which is different to your QMUL account used to login to your managed device. When you first receive your loan laptop, a member of ITS will help you set your local account password. This password should be different to any of your personal or work passwords. When you return from your trip, you should return your device to ITS as soon as possible. Please do not use your loan laptop once you have returned to the UK.

2. **Accessing QMUL services via the browser**

Wherever possible you should use Zoom, Teams, and Outlook via a browser, since this will minimise the amount of data downloaded and stored on your laptop. The recommended browsers to use are Google Chrome, Microsoft Edge, or Mozilla Firefox.

- To access your QMUL email and calendar in your browser, navigate to [https://mail.qmul.ac.uk](https://mail.qmul.ac.uk).
- To access your QMUL Teams account in your browser, navigate to [https://teams.microsoft.com/](https://teams.microsoft.com/).
- To access your Microsoft Office 365 applications in the browser (Word, PowerPoint, Excel, etc), navigate to [https://www.microsoft365.com/](https://www.microsoft365.com/).
- To access your files in SharePoint and OneDrive in your browser, navigate to [https://qmulprod-my.sharepoint.com/](https://qmulprod-my.sharepoint.com/).
- To access your Zoom account in your browser, navigate to [https://zoom.qmul.ac.uk/](https://zoom.qmul.ac.uk/).

If there are performance issues with the browser version, then section 3 contains guidance on how to login to the full desktop client applications. Please only use the desktop versions if the web browser performance makes it unsuitable for your work.

2.1 **Joining meetings via a browser**

To join a Zoom/Teams meeting, you can either navigate to your Teams/Zoom account at the links above and join the meeting, or you can click the meeting link in the email invite, which will open the meeting in your browser by default.

2.2 **Logging into QMUL accounts**

When you access your QMUL email, Teams, or Zoom accounts, or the Office 365 services, via the web browser, you will be asked to enter your username (abc123@qmul.ac.uk) and password. You will then be prompted to enter the two-factor authentication numbers. Leave the ‘Don’t ask again for 30 days’ box unchecked and then confirm the two digits in your authenticator app. You will then be logged into your QMUL account.
2.2.1 **Microsoft Authenticator App**

If you normally use the Microsoft authenticator app as your second factor authentication method you will need to ensure you bring the mobile device with the app installed with you, or you will not be able to access your accounts.

If you decide to take a separate phone with you, then you must install the Microsoft authenticator app on this phone and link it with your QMUL account before you leave the UK. Please see the guidance below for how to add an authenticator app to your account.

**Multi-Factor Authentication (MFA) - IT Services (qmul.ac.uk)**

2.3 **Border Crossings**

Prior to going through customs at a border crossing you should ensure you are logged out of all your accounts, both on the web browser and desktop clients (if you have used them).

2.3.1 **Logging out of browsers**

To log out of accounts you have accessed through the browser please follow the guidance below for each browser you have used to access your QMUL account:

- **Microsoft Edge**: In Edge navigate to edge://settings/clearBrowserData. Change the time range to ‘all time’ and make sure that ‘Cookies and other site data’ is selected. Then click ‘clear now’.
- **Google Chrome**: In Chrome navigate to chrome://settings/clearBrowserData. Change the time range to ‘all time’ and make sure that ‘Cookies and other site data’ is selected. Then click ‘clear data’.
- **Mozilla Firefox**: In Firefox navigate to about:preferences#privacy. Find the ‘cookies and site data’ section and click ‘clear data’. Make sure ‘cookies and site data’ is selected. Then click ‘clear’.

2.3.2 **Logging out of applications**

If you need to use the full desktop client for any applications, please make sure you have logged out of each application prior to travelling through customs.

- For Microsoft Teams and Office 365 applications, open the main page of the application and select your initials in the top right corner. Then click ‘Sign out’.
- For Zoom, click your profile picture/icon in the top right corner and select ‘sign out’.
• For Outlook, select ‘file’ in the top right corner, then select ‘account settings’ and ‘account settings’ again from the drop down. In the pop up, select the data files tab and click add, then click OK (the name is not important). Then select the email tab, select your email address, and click remove.

3. **Full client access**

If using Zoom, Teams, or Outlook via a browser connection does not provide a usable service, then open the ‘full’ versions of the application from the start menu, as you would on your usual QMUL device. As with the browser version, you will need your university credentials and two-factor authenticator app to hand to login to the Outlook, Teams, or Zoom desktop applications. It is recommended that you test this functionality before you leave the UK and ideally from a non-University network. Once you have tested, please ensure you sign out of any full clients you have accessed before travelling.

When logging into any Microsoft applications such as Teams, Outlook, or Office 365, you will be asked if you want Windows to ‘automatically sign you into all your applications’, please select ‘No, sign into this app only’ when you are prompted to minimise the number of desktop applications you are logged in to.

3.1 **Teams**

1) Enter your email address (ab123@qmul.ac.uk).

2) When you login you might need to enter your two-factor authentication code. This will either be via the authenticator app, or via an emailed code. If it is via the app then, please refer to the instructions in section 2.2. If it is an emailed code, please follow the instructions below.

3) Click on Send Code
4) Enter the code sent to your email.

5) Once you have entered your two-factor authentication you will be asked if Windows should remember your account. Click on 'No, sign into this app only'.
3.2 Outlook

1. Open Outlook and select File > Add Account.

2. If you haven't launched Outlook before, you'll see a welcome screen.
3. When prompted, enter your email address, and select 'Connect'.

![Outlook](image)

Email address
---
Email address

Advanced options

Connect

No account? [Create an Outlook.com email address to get started.](#)

4. If your screen looks different, enter your name, email address, and password, and select Next.
5. If prompted, enter your password, and select OK.

3.3 **Zoom**

1. Open the Zoom application and click on Sign In.
2. Choose the Sign in with SSO option.
3. Enter ‘qmul-ac-uk’ as the company domain and click continue.

4. This will open a browser window where you will be asked to enter your QMUL email (ab123@qmul.ac.uk) and password. If asked to enter your two-factor authentication, then please follow the instructions in section 2.2.

5. You will then be logged into your QMUL Zoom account.
Loan PC and Traveller Policy Acceptance Form

Date: __________________________________________________________

First Name: ____________________________________________________

Surname: _______________________________________________________

School / Department: ____________________________________________

<table>
<thead>
<tr>
<th>Service Request Number</th>
<th>Item Description</th>
<th>Asset Tag</th>
<th>Expected Return Date</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

The recipient of the above Loan PC is responsible for keeping the device and its content safe and secure.

The recipient agrees not to use the Loan PC upon return from the High-Risk country and to return the equipment to the IT Service Desk or School IT representative for wiping and rebuild immediately upon return from travel.

The recipient agrees to return all associated equipment (mouse, power pack, etc.) when returning the Loan PC.

The recipient hereby accepts the conditions as set out in the Staff Travelling to High-Risk Countries Policy.

Print Name: ____________________________________________________

Signature: _____________________________________________________

Date: __________________________________________________________

*Items must not be handed over if the recipient does not hold a valid QMUL ID Card.*

*Two copies, one for the customer and one for IT Service Desk / School IT representative.*