Information and Cyber Security Requirements for International Travel

Version:	1.0
Dated:	21/07/2026
Document Owner:	Head of IT Security Operations

Document History and Reviews

Version	Date	Revision Author	Summary of Changes
0.1	30/06/2026	Matt Harvey	Standard creation
1.0	07/07/2026	Matt Harvey	Minor changes suggested by ITOB

Review Distribution

Name	Title
IT Operating Board	

Initial Approval

Versions	Position and Comments	Approved Date
1.0	IT Operating Board	07/07/2026

Final Approval

Versions	Position	Approved Date
1.0	ISG	21/07/2026

Contents

Purpose

This policy defines the information and cyber security requirements for staff and associates travelling internationally on behalf of the University. It aims to protect University information, research, systems, services and devices from the increased security risks associated with overseas travel.

This policy supplements the University's Travel Policy by defining the mandatory information and cyber security requirements that apply before, during and after international travel on University business. It does not replace the University's travel approval, insurance or health and safety requirements.

The policy adopts a risk-based approach to international travel. Whilst all overseas travel requires appropriate information and cyber security precautions, additional mandatory controls apply when travelling to designated high-risk countries where there is an increased risk of cyber compromise, device exploitation, surveillance, or unauthorised access to University information.

This policy supports the University's legal, regulatory and contractual obligations for protecting information and is based on recognised UK good practice, including guidance published by the UK National Cyber Security Centre (NCSC) and Jisc on cyber-secure international travel.

Scope

This policy applies to University staff, associates and students travelling internationally on University business where they will:

- Use University-issued or personal devices to access University systems or services.
- Access, process, store or transmit University information whilst overseas.
- Carry University information, research data, intellectual property or personal data during travel.

This policy applies to all international travel undertaken on behalf of the University where access to University information, systems or services is required. Additional mandatory controls apply when travelling to designated high-risk countries requiring enhanced security controls.

This policy covers:

- The use of University-issued devices and approved travel devices for international travel.

- The use of personal devices where they may access University systems, services or information.
- Identity, authentication and secure access to University systems and services.
- The handling, storage, transmission and protection of University information whilst travelling.
- The reporting of lost, stolen or compromised devices, accounts or University information.

Related Policies and Guidance

This policy should be read in conjunction with the following University policies, standards and guidance:

- University Travel Policy
- IT & Information Security Policies
- IT Regulations
- Information Classification and Handling Policy
- Data Protection Policy
- Incident Management Policy

Roles and Responsibilities

Staff and Associates

Staff and associates travelling internationally on University business are responsible for:

- Complying with this policy and any associated standards or guidance.
- Completing any required travel risk assessments.
- Seeking advice from IT Services or IT Security where required, particularly when travelling to countries requiring enhanced security controls.
- Using University-issued devices and services in accordance with this policy.
- Protecting University information, devices and credentials throughout the period of travel.
- Promptly reporting the loss, theft or suspected compromise of any device, account or University information in accordance with the University's incident reporting procedures.

Line Managers

Line managers are responsible for:

- Ensuring staff are aware of this policy before undertaking international travel.
- Ensuring that appropriate travel and information security risks have been considered as part of the travel approval process.
- Supporting staff in complying with this policy where additional security measures are required.

IT Services and IT Security

IT Services and IT Security are responsible for:

- Maintaining this policy and associated guidance.
- Identifying countries requiring enhanced security controls, taking account of advice from the Foreign, Commonwealth & Development Office (FCDO), the National Cyber Security Centre (NCSC), Jisc and other relevant threat intelligence.
- Providing advice to staff and associates on secure international travel.
- Providing and managing approved travel devices and technical controls where required.
- Responding to reported information security incidents associated with international travel.

Countries Requiring Enhanced Security Controls

The University has identified the following countries as requiring enhanced information and cyber security controls. This designation is informed by advice from the Foreign, Commonwealth & Development Office (FCDO), the National Cyber Security Centre (NCSC), Jisc and other relevant threat intelligence:

- China
- Iran
- North Korea
- Russia

These countries have been identified as presenting an increased risk of cyber compromise, device exploitation, surveillance, unauthorised access to University systems or information, and the interception of electronic communications.

For travel to these countries, staff and associates must comply with the enhanced security requirements defined within this policy. These requirements include the mandatory use of University-issued travel devices, restrictions on the use of personal devices, and additional controls governing access to University systems, services and information.

The list of countries requiring enhanced security controls is maintained by IT Security and is informed by advice from the UK Foreign, Commonwealth & Development Office (FCDO), the National Cyber Security Centre (NCSC), Jisc and other relevant threat intelligence. The University reserves the right to amend this list in response to changes in the threat landscape.

Planning and Approval

Information and cyber security considerations must form part of the planning process for all international travel undertaken on University business.

Before travel is approved, staff and associates must:

- Complete the University's required travel approval and risk assessment processes.
- Consider the information and cyber security risks associated with the destination, the purpose of travel, the information being accessed or carried, and the systems that will be used.
- Ensure that only the minimum access to University systems, services and information necessary for the purpose of the trip is required.
- Notify the University's IT support arrangements at least two weeks before departure where travel involves a country requiring enhanced security controls, or where advice is required on the secure handling of University information or systems.

Where travel is to a country requiring enhanced security controls, staff and associates must engage with IT Services sufficiently in advance of travel to allow appropriate security measures to be implemented. This includes the provision of approved travel devices and any additional technical controls required by this policy.

Travel should not proceed until the required information and cyber security arrangements have been agreed and implemented.

Preparing for International Travel

Before undertaking international travel on University business, staff and associates must ensure that appropriate information and cyber security controls are in place to protect University information, systems and devices.

Requirements for all International Travel

Prior to travel, staff and associates must:

- Complete the University's required travel approval and risk assessment processes.
- Ensure any University-issued device used during travel is fully updated with the latest operating system and security patches.
- Ensure full disk encryption is enabled on University-issued laptops and mobile devices.
- Use University-approved Multi-Factor Authentication (MFA) to protect access to University systems and services.
- Take only the minimum University information and data necessary for the purpose of the trip.
- Store University information only within approved University systems and services.
- Ensure they understand the University's procedures for reporting lost, stolen or compromised devices, accounts or information.
- Please seek advice from IT Services or IT Security where additional guidance is required or any calcifications on the points above.

Additional Requirements for Countries Requiring Enhanced Security Controls

Staff and associates travelling to countries requiring enhanced security controls must:

- Use only University-issued travel laptops and mobile phones provided specifically for international travel.
- Use only approved travel devices configured by IT Services for high-risk travel.
- Ensure travel devices contain only the minimum software, accounts and University information necessary for the duration of the trip.
- Remove University accounts, applications and synchronised University data from personal devices before departure.
- Not take their standard University-issued laptop or mobile phone unless explicitly authorised by IT Security.
- Engage with IT Services sufficiently in advance of travel to allow travel devices and security controls to be prepared and tested.

Working Securely Whilst Abroad

Whilst travelling internationally, staff and associates must take appropriate steps to protect University information, systems and devices.

This includes:

- Accessing University systems only through University-approved secure remote access methods and encrypted connections.
- Using only University-approved authentication methods when accessing University services.
- Avoiding the use of public or shared computers to access University information overseas.
- Keeping devices under their personal control wherever possible and never leaving them unattended in public places.
- Locking devices whenever they are unattended, even for short periods.
- Avoiding the connection of unknown USB devices, storage media or charging equipment to University devices.
- Avoiding the discussion or display of sensitive University information in public environments where it may be overheard or observed.
- Exercising particular caution when using public Wi-Fi networks and following IT Services guidance regarding secure network access.
- Immediately reporting the loss, theft or suspected compromise of any device, account or University information in accordance with University incident reporting procedures.

Returning from International Travel

Following international travel, staff and associates must ensure that any temporary security arrangements implemented for the trip are appropriately concluded.

Where travel involved a country requiring enhanced security controls:

- University-issued travel devices must be returned to the IT Services as soon as reasonably practicable following return to the UK.
- Travel devices must not be connected to the University network or used to access University systems after returning to the UK.
- Travel devices should not be powered on used after returning to the UK unless instructed to do so by IT Services.
- Any suspected information or cyber security incident identified during or after travel must be reported immediately.
- Staff and associates must cooperate with any post-travel security review.

Returned travel devices will be assessed, securely wiped and reconfigured before being returned to service or reissued for future travel.

Incident Reporting

Any actual or suspected information or cyber security incident occurring before, during or after international travel must be reported to the University as soon as possible.

Examples include, but are not limited to:

- Loss or theft of a University-issued or personal device used to access University systems.
- Suspected unauthorised access to a device, account or University information.
- Unexpected requests to inspect, access or retain a University device.
- Loss, disclosure or compromise of University information.
- Suspected phishing, credential theft or compromise of authentication methods.
- Any other event that may affect the confidentiality, integrity or availability of University information or systems.

Staff and associates must follow the University's Information Security Incident Management procedures and cooperate fully with any subsequent investigation undertaken by IT Security or Information Governance.

Exceptions

Exceptions to this policy will only be granted where there is a clear business justification and the associated information and cyber security risks have been assessed and accepted.

All exceptions must:

- Be documented and supported by an appropriate risk assessment.
- Be approved by IT Security and, where appropriate, the relevant business owner.
- Define any compensating controls required to reduce the identified risks.
- Be time-limited and subject to periodic review.

Where an exception cannot adequately reduce the identified risks, the University reserves the right to prohibit the proposed travel arrangements or access to University systems and information.

Compliance and Monitoring

Compliance with this policy will be monitored through the University's information security governance and assurance processes.

These may include:

- Review of travel requests involving countries requiring enhanced security controls.
- Verification that appropriate travel devices and security controls have been provided where required.
- Review of approved exceptions and associated risk assessments.
- Post-travel confirmation that temporary travel devices have been returned and appropriately reconfigured.
- Review of information and cyber security incidents associated with international travel.

Failure to comply with this policy may increase the risk of unauthorised access to University information and systems and may be managed in accordance with the University's disciplinary procedures, contractual obligations or other applicable policies.

Review

This policy is owned by IT Services and will be reviewed by IT Security at least annually, or sooner where required to reflect:

- Changes to the University's risk appetite or governance requirements.
- Changes to legislation, regulatory obligations or contractual requirements.
- Updates to guidance issued by the National Cyber Security Centre (NCSC), Jisc or the Foreign, Commonwealth & Development Office (FCDO).
- Significant changes to the international threat landscape or emerging information and cyber security risks.
- Lessons identified from information or cyber security incidents relating to international travel.

Any material changes to this policy will be approved in accordance with the University's policy governance arrangements.