Devices for International Travel Procedure	
Enabling Policy Statement; Executive Owner; Approval Route:	Our Data - Chief Operating Officer - Compliance Committee
Is the Procedure for internal use only (Non-disclosable) ?	Disclosable
Associated Policy Statements:	Our Partnerships & Reputation - VP Global
Authorised Owner:	Chief Information Security Officer
Authorised Co-ordinator:	Lead Information Security Assurance Specialist
Effective date:	05/03/2024
Due date for full review:	04/03/2025
Related documentation:	Procedure for Collaborating with Sensitive Jurisdictions Our Data Policy Statement Acceptable Use Policies Statement Using Your Own Applications and Devices Policy Security-sensitive Research Policy Staff Travel and Expenses Procedure Academic Technology Approval Scheme (ATAS) Export Controls Policy Terms of Reference: Compliance (Data) Committee / Partnerships and Reputation Committee

Approval History

Version	Reason for review	Approval Route	Date
1.0	First major version	Compliance (Data) Committee	05/02/2024

1. Purpose

1.1. Mobile devices such as laptops, smartphones and tablets, along with organisational cloud services, remote connections to enterprise networks and databases, facilitate work during international travel. However, mobile devices are particularly susceptible to compromise, theft, physical damage, and loss, regardless of user location. Use of mobile devices during international travel can intensify this risk, so you should take steps to ensure that University of Surrey data is not irrecoverably lost, and to prevent confidential data falling into the wrong hands.

1.2. When planning international travel for University business it is important to consider how you can securely access information from your devices. This document summarises best practices to ensure data is protected before, during, and when you return from your travel abroad.

2. Scope and Exceptions to the Procedure

2.1. The security guidance herein applies to:

- All staff using University of Surrey mobile devices (laptops and mobile phones) as they travel internationally
- All University of Surrey data including personal data
- The equipment, systems, credentials, etc. that are used to access and safeguard data

2.2. Failure to comply may lead to:

- Damage and distress being caused to those who entrust us to safeguard their data
- Reputational damage to the University and its relationship with stakeholders
- Damage caused by unavailability, inaccessibility or corruption of University Information Assets
- Disciplinary action being taken against members of staff up to and including dismissal. In the case of a breach of this policy by a contractor, it may lead to termination of the engagement or referral for action under other procedures

3. Definitions and Terminology

Data - information in all its forms which is under the control of the University

Encryption - the process of encoding data, information or messages in a way that is only accessible by authorised persons who hold the related keys to permit decryption

Information - see “Data”

Personal data - any information that relates to an identified or identifiable living individual

Information classification – see IAO Handbook

Sensitive jurisdictions – see Procedure for Collaborating with Sensitive Jurisdictions

4. Procedural Principles

Responsibilities

4.1. Overall responsibility for the University’s strategic plans for information security rests with the Executive Board member serving as the Chair of Compliance (Data).

4.2. The Chief Information Officer is responsible for ensuring that the arrangements for governing the scoping, development, implementation and maintenance of University IT systems, networks and databases comply with the principles of good information security. This includes the delivery of resources for secure access to University resources for staff travelling on University business through high-risk and other territories.

4.3. Responsibility for the identification, treatment and remediation of information risk, including both those within the orbit of IT Services as well as those across the rest of the University resides with

the Chief Information Security Officer.

4.4. Information Asset Owners are accountable for ensuring that information assets within their realm of responsibility are managed in accordance with the Our Data Policy Statement, legislative context, and any contractual agreements involving third parties.

4.5. All staff who are users of information systems must manage the creation, storage, amendment, copying, archiving and disposal of information in a manner which safeguards and protects its confidentiality, integrity and availability. This includes staff planning international travel on behalf of the University.

4.6. All staff are responsible for accessing and engaging with all information security training and guidance provided by the University.

Before you travel

4.7. IT Services recommends bringing only the equipment needed to do your work while travelling. Below you will find device recommendations that range from the minimum required actions to the best, most secure options that help keep devices secure and data protected.

4.8. No personal data (e.g. related to staff, students, research participants etc) should be taken outside the EEA without prior consultation with the Information Governance team. Similarly, if you have any questions about the destination country's approach to equality, diversity and inclusion, please consult with the EDI team ahead of travel.

4.9. For travel to countries not considered Sensitive Jurisdictions, be sure to follow these additional steps before you go:

Laptops:

4.9.1. Remove any documents containing proprietary or confidential University information (including customer data), research data, intellectual property or personal data from your device/s. If you believe that you need to travel with local copies of data in any of these categories, first contact the Information Governance team for guidance.

4.9.2. Verify that your computer software is supported and has received the most recent security patches available. Seek guidance from IT Services, if unsure.

4.9.3. Unless travelling to a region covered in https://www.comparitech.com/blog/vpn-privacy/encryption-laws/ , verify that your laptop is encrypted.

4.9.4. If challenged at border controls, you should ensure that the device has power and any usernames or passwords are readily available to assist in unlocking the device or accessing the data.

4.9.5. Leave USB drives at home. These are easily lost and easily corrupted. If you must travel with a USB device, be sure that it is encrypted. Seek guidance from IT Services, if unsure.

Mobile Devices:

4.9.6. Remove any documents containing proprietary or confidential University information (including research data, intellectual property or personal data) from your device/s. If you believe that you need to travel with local copies of data in any of these categories, first contact the Information Governance team for guidance.

4.9.7. Verify that your phone software is supported and has received the most recent security patches available.

4.9.8. If travelling with an organisationally-issued phone, confirm with IT Services team that the device is enrolled for central management, encrypted and/or capable of being remotely wiped. It is recommended to minimise the amount of data carried on any mobile device while travelling.

Account Security:

4.9.9. Ensure that your account is set up for self-service password reset at https://mysignins.microsoft.com/security-info as per these instructions. This is an important measure since account recovery via secondary email accounts may not be possible in countries where certain common email services such as Google Mail are unavailable.

Enhanced Security: Travel with a device built to Travel Loaner standards

4.10. Where staff are travelling to a country categorized as a Sensitive Jurisdiction by Research and Innovation Services, an International Travel Risk Assessment shall be undertaken (this can be found at: https://travelriskassessment.surrey.ac.uk) and Travel Loaner devices requested. You should complete a Travel Risk Assessment before each International trip and the form will be updated to reflect latest guidance from Research and Innovation Services. Privacy screen filters will be made available alongside travel laptops.

4.10.1. Where a Travel Loaner laptop is unsuitable e.g. a specific software is not operable on a loan device, an agreed exemption from an Associate Dean Research and Innovation, or a member of Executive Board (for professional services), or the Vice Chancellor (for a member of the Executive Board), will be required before travelling with your own standard University device.

4.11. Through the Travel Loaner Program, you can borrow an unencrypted laptop with minimal software footprint to use instead of your own computer, and a temporary mobile phone can also be issued. The Travel Loaner device will allow you to manage email, view your calendar, run presentations, edit documents, and connect to University websites, but is also designed to minimise the information to be stored locally on the device. The device will be set up specifically for your travel, then wiped back to factory settings when you return. This is also a requirement of some specific research grants.

4.12. Where identified through the International Travel Risk Assessment or other contractual requirement, staff should request a Travel Loaner laptop and mobile phone via the IT Request Forms page on Surreynet, at least 10 days ahead of their date of travel, to allow sufficient time for the new device deployment.

4.13. Travellers to Sensitive Jurisdictions should expect their devices (phones, laptops, tablets, etc.) to be openly examined and scrutinized by immigration officials and perhaps local law enforcement. They may be expected to supply officials with a password to unlock their device and provide access to any local data, and failure to do so could result in the device being confiscated as well as possible detention or expulsion from the country. The provision in this area has therefore been developed to reduce the personal risk to University of Surrey staff undertaking international travel.

While you travel

4.14. The following is general advice, whether travelling with a Travel Loaner device or a standard-issue University of Surrey computer:

Dos

- Be aware of your surroundings. Watch for those looking over your shoulder or potential thieves
- Disable broadcast services like Wi-Fi access points, Bluetooth devices, and GPS when not needed
- Use private browsing whenever possible (Chrome, Firefox, Safari, Edge)
- If your device(s) are lost or stolen, immediately:
  - Report to University Information Governance team at Report a breach
  - Submit a ticket for lost or stolen mobile devices to itservicedesk@surrey.ac.uk
- Connect devices only to authorised computers and peripherals
- Keep all software (including both operating systems and applications) up-to-date
- Use strong lock-screen PINs/passwords (minimum 6-digit)

Don'ts

- Do not assume public power charging services such as kiosks are safe and free of compromise; use your own power chargers where possible
- Avoid using public workstations as they cannot be trusted. Assume that anything that you enter into the public workstation may be captured
- Do not leave your devices unattended. Even hotel safes may not be secure
- Avoid connecting to untrusted resources such as public Wi-Fi access points and Bluetooth devices
- Do not click on any unknown web links sent via e-mail or text messaging
- Do not attempt to circumvent restrictions on UoS-issued devices

4.15. Please note that the University of Surrey VPN is strictly geofenced based on risk-assessment, so is unavailable from most international destinations. Other services such as the University's Virtual Desktop service permit remote access to internal University of Surrey resources without specific geographical restrictions.

After you travel

4.16. For users returning from high-risk territories (Sensitive Jurisdictions) or those who have been issued a Travel Loaner device for other reasons:

- Avoid immediately reconnecting Travel Loaner devices to personal or University networks as the device should be treated as untrusted
- As part of return of the Travel Loaner device service, it will be wiped and redeployed as an anti-malware measure

Import and Export Controls related to Encryption

4.17. Please consult the University's Export Controls Policy.

4.18. Whilst many countries allow visitors to bring portable devices through border controls unchallenged, some countries try to restrict the use of encryption and require the possession of appropriate import/export licences. Attempting to take encrypted data or devices to these countries without obtaining licences may result in the device being confiscated or other penalties including imprisonment.

4.19. While "personal use exemptions" which allow individuals to enter countries with encrypted data or devices without the need for a licence, it is better to check with the country you're travelling to beforehand https://www.comparitech.com/blog/vpn-privacy/encryption-laws/. Remember, even though you may not need a licence to take encrypted data or devices into a country, upon entry, you may still be asked to disclose the data, so it's safest not to take personal or sensitive data with you.

4.20. If a country requires an import licence, these are usually obtained by applying to the government of the country in question. The following website provides the contact details for some countries: https://www.wassenaar.org/participating-states/. Be aware, that even with a licence, your laptop may still be searched and you may be asked to decrypt it.

4.21. The provision of an unencrypted Travel Loaner laptop with a minimal software footprint, designed to discourage local storage of data, is offered in order to simplify encryption concerns related to travel through Sensitive Jurisdictions. If in doubt, contact trustedresearch@surrey.ac.uk for further guidance.

Reporting security concerns

4.22. All security incidents, including actual or potential unauthorised access to University of Surrey information systems should be reported immediately at https://www.surrey.ac.uk/information-governance/report-data-breach

5. Governance Requirements

5.1. Implementation: Communication Plan

5.1.1 This Procedure is communicated to all staff as part of the University Policies and Procedures website.

5.1.2 Socialisation through appropriate structures and groups at faculty level, including staff and students as relevant.

5.2 Implementation: Training Plan

5.2.1 All Process Steps emphasis and signpost sector guidance and training available on the Trusted Research SharePoint pages.

5.2.2 From time-to-time the Partnership and Reputation Committee will mandate obligatory training is undertaken such as Export control training by individual or groups of staff and/or students.

5.3 Review

This Procedure is regularly reviewed by Partnerships and Reputation Committee. Minor changes will be reviewed and agreed by PRC. Major changes will be reviewed through PRC and submitted to Council for noting. Review will typically be every three years unless legislative changes require earlier major changes.

5.4 Legislative Context and Higher Education Sector Guidance or Requirements

- The General Data Protection Regulation 2016/679
- The Data Protection Act 2018
- The Freedom of Information Act 2000
- The Computer Misuse Act 1990
- The Counter Terrorism and Security Act 2015 (in particular the Prevent Duty)
- The Payment Card Industry Data Security Standard (PCI DSS)
- Copyright, Designs and Patents Act 1988

5.5 Sustainability

This procedure has no impact on carbon emissions or on energy consumption.

6 Stakeholder Engagement and Equality Impact Assessment

6.1. An Equality Impact Assessment was completed on 06/02/2024 and is held by the Authorised Owner.

6.2. Stakeholder Consultation was completed, as follows:

Stakeholder	Nature of Engagement	Request EB Approval (Y/N)	Date	Name of Contact
Governance	Procedure review		26/01/24	Kelley Padley
H&S	Procedure review		09/01/24	Matthew Purcell
Sustainability	Procedure review		26/01/24	Martin Wiles
EDI Team	Procedure review		26/02/24	Jo McCarthy-Holland
Our Partnerships & Reputation	Procedure review and feedback at PRC on 11.01.24 and 05.03.24			Patrick Degg