HOUSES OF PARLIAMENT
RESTORATION & RENEWAL

Data and Digital Overseas Travel Policy

R&R Digital Service

Table of Contents

1 Introduction

1.1 Purpose

From time to time, R&R Data and Digital Subscribers may be required to travel outside of the United Kingdom (UK) for business or personal reasons. However, travelling with a laptop or mobile device significantly increases the possibility of data/identity theft and the introduction of malware. Travel to some countries and geographic regions also carries a significantly higher risk than others. Government Agencies within some countries are known to routinely monitor airport, hotel and other public electronic communication.

R&R Data and Digital Customers should also be aware that not all countries permit the freedom of digital experience that we have in the UK, and that it may as a visitor be illegal to access certain sites and/or services.

For these reasons, this policy describes the R&R Programme controls to safeguard the security and integrity of R&R Data and Digital Services.

1.2 Scope

This policy is applicable to all R&R Data and Digital Devices. It is also applicable to bring your own devices (BYOD) e.g. laptops, tablets and mobile phones used by R&R Data and Digital Customers to access R&R digital services and data while travelling.

1.3 Governance and Review

This Policy, particularly the list of Restricted Countries, will be reviewed and updated as and when new travel advice is issued by the UK government. The policy will also be reviewed twice annually to incorporate feedback, lessons learnt and any other required changes.

Changes will be made by the Policy Owner, assured by the R&R Data and Digital Senior Leadership Team and approved by Sponsor Body CEO or authorised delegate.

2 Policy Compliance

While some aspects of this Policy will depend on the nature, scope and owner of particular data and devices and the country of travel, compliance with this Policy is mandatory for all R&R Data and Digital Customers. Where appropriate, and at the discretion of the R&R Digital Service Centre (DSC) Lead and DSC Operations Lead, non-compliance exceptions may be granted on a case by case basis where explicitly requested in advance of travel.

3 Related Documents

1. R&R Acceptable Use of Digital Services Policy

4 Definitions

Term	Meaning
Restricted Country	Countries listed in Appendix A of this document.
Non-Restricted Country	Any country not listed in Appendix A of this document.
Transit	Any form of land-based presence during travel including airport transfers, car, coach and foot travel.
Digital Device	Laptops, tablets and mobile phones.
Digital Device Accessories	Including but not limited to mice, cables, bags, privacy screens, Surface Pens, power and display adapters.

5 Policy Statements

5.1 R&R Data and Digital Devices

i. R&R Data and Digital devices must not be taken for personal or R&R business travel reasons by R&R Data and Digital Customers visiting or transiting through Restricted Countries.
ii. R&R Data and Digital Customers may take and use R&R Data and Digital Devices in Non-Restricted Countries subject to compliance with this Policy.
iii. R&R Data and Digital Customers are responsible at all times for the physical security of R&R Data and Digital Devices. These must not be left unattended at any time while travelling, particularly in public places such as airports, train stations, hotels, restaurants, and bars.
iv. R&R Data & Digital Devices must not be left in hired vehicles at any time but should instead be carried by the customer when leaving the vehicle unattended.
v. R&R Data and Digital Devices must be kept in hand luggage rather than checked in luggage.
vi. When not in use, R&R Data and Digital devices should be kept in a secure location such as a hotel safe.
vii. If an R&R Data and Digital Device is lost or stolen while travelling, both within and outside of the UK, the R&R Data and Digital Service Centre must be informed as soon as possible so that the device(s) can be remotely disabled and wiped.
viii. Loss or theft of an R&R Data and Digital Device, in any country, must be reported to local police as soon as possible and a copy of the loss/theft report provided to the Digital Service Centre as soon as possible. .

5.2 Bring Your Own Device (BYOD)

i. Before travelling with BYOD devices, R&R Data and Digital Subscribers must ensure that they are updated with the latest manufacturer Anti-Virus and OS patches. If in doubt, contact the Digital Service Centre for guidance.
ii. R&R Data and Digital Services must not be accessed via BYOD devices for any reason while in Restricted Countries.

iii. Loss or theft in any country of a BYOD device, that is being used to access R&R Data and Digital Services, must be reported to the Digital Service Centre as soon as possible.

5.3 General Principles

i. R&R Data and Digital Customers are personally responsible for ensuring that they comply with any international sanctions and local law applicable to the country of travel.
ii. Personal safety should be the highest priority at all times. R&R Digital Customers should avoid using BYOD and R&R Data and Digital devices in areas where it may attract unwanted attention. If threatened, R&R Data and Digital Customers should not attempt to prevent theft of Data and Digital devices.
iii. Caution should be exercised when using Data and Digital devices in public places where screen content could be seen or conversations overheard.
iv. R&R Data and Digital Customers must also inform the Digital Service Centre as soon as possible if they suspect that an R&R Data and Digital device or BYOD device may have been compromised, e.g. they have been removed for inspection by a Foreign Agency, security service or lost/stolen and then recovered. No further access of R&R Data and Digital Services may be made until approved by the Digital Service Centre.
v. R&R SharePoint or OneDrive must be used for all file storage. Documents and files must not be stored locally on devices (e.g. hard disks) or on any portable storage devices (e.g. USB drives, CD ROMs etc).
vi. Document links rather than file attachments should be used when sharing data and files via email.
vii. Documents, emails or any other form of electronic data must not be printed while travelling within Restricted and Non-Restricted Countries.
viii. Wi-Fi connection and access to online services (email, Office 365, SharePoint etc.) in the non-restricted Countries, must be made via the installed VPN application installed on R&R Data and Digital devices.
ix. R&R Data and Digital Customers should assume that all electronic communication made via BYOD and R&R Data and Digital devices are being monitored by Foreign Security Services and Corporations.
x. Documents classified as Official, and emails classified as Unrestricted or Restricted, may be created and edited in Non-Restricted Countries subject to compliance with all other clauses of this policy.
xi. Documents classified as Secret or above, and emails classified as Highly Restricted, must not be accessed in any way (e.g. viewed, edited, saved, deleted) when travelling overseas.

6 Training Requirements

Customers will be given a copy of this Policy as part of their welcome email. It is the Customer's responsibility to read and understand the Policy.

Periodic training will be given to customers to enhance their understanding.

7 Monitoring and Compliance

Compliance with all responsibilities will be audited. This may be performed manually, through ad-hoc activities or via automated capture of data, e.g. completion of Cyber Security training, attempts to access restricted sites, etc.

Unintentional non-compliance will not normally require any action, except for further education of the Customer.

Intentional non-compliance is more serious and appropriate action will be taken on a case by case basis. Consequences of data and digital breach may include, but are not restricted to:

- escalation to the Customers line manager,
- possible restriction in accessing the R&R Digital Service; and/or
- disciplinary sanctions or action,

and in extreme cases:

- civil action against the Customer and/or their employer; and/or
- notification to the appropriate authorities that there has been a crime or regulatory infringement.

8 Associated Documentation

R&R Data & Digital Service Acceptable Use Policy

R&R Data and Digital Travel Policy

The Parliamentary Digital Service also has standards and policies relating to the use of their services and data. These should be referred to should a Customer require access to its service offerings. This is not connected to, and has no bearing on, the R&R standards and policies.

9 Equality Assessment

An Equality Assessment has been performed against this document and can be found in Equality Analysis D&D Travel Policy available from R&R D&D Communications.

Sarah Johnson
On behalf of the Sponsor Body
August 2020

David Goldstone
On behalf of the Delivery Authority
August 2020

Appendix A – Restricted Countries

Transport, personal or on behalf of R&R, of any R&R Data and Digital devices and mobile phones to the countries listed below is not permitted.

Afghanistan	Algeria	Belarus
Burundi	Cameroon	Central African Republic
Chad	China, The People's Republic of	Colombia
Congo, Democratic Republic of the	Crimea (Region of Ukraine)	Cuba
Egypt	El Salvador	Eritrea
Haiti	Honduras	Hong Kong
Iran*	Iraq	Israel, the West Bank and Gaza
Kenya	Korea, Democratic People's Republic of*	Lebanon
Libya	Mali	Mauritania
Mexico	Myanmar	Niger
Nigeria	Pakistan	Philippines
Russia	Saudi Arabia	Somalia
South Sudan, Republic of	Sudan	Syria
Thailand	Ukraine	Venezuela
Yemen	Zimbabwe	