

BC7: Working from Abroad Procedure

January 2023

Owner: Information Governance Board for CLT

Version: 1.8

Date created: March 2022

Last Review January 2023

Next Review date: March 2023

Be aware that any printed copies of this document may not be the most recent version. Please check on the Intranet to ensure that you are using the current version before relying on the information contained within it.

NOTE in relation to this procedure:

This Procedure forms part of the Council's Information Governance Framework covering all aspects of Information Governance and Management, Data Protection, Information Security and Cyber Security. Please note that this procedure combines IG, Information Security, Insurance, and HR requirements.

Version	Date Reviewed	Summary of Changes	Updated by	Approved by	Date Published	Published to
1.0	22/01/22	New procedure created	Alexandra West/ Chris French			
1.0	14/02/22	HR additions	LD/RE			
1.1	16/02/22	IT additions	Phillip Cooper			
1.2	18/02/22/	IT/HR additions merged	LD/PC			
1.3	21/02/22	IG Final corrections	AW			
1.4	31/03/22	CLT Approved Procedure	CLT	CLT	April 2022	IG/IT/HR intranet pages
1.5	19/12/22	Amended IT Service Desk Links.	Phillip Cooper	FA/AU	19/12/2022	IT Application / forwarded to IT and IG.
1.6	19/12/22	Removed Risk Assessment questions from this document and included link to RA form	Peter J Streatfield	PC	19/12/2022	IT Application / forwarded to IT and IG.
1.7	03/01/23	Added Japan, Israel and Uruguay to green list following review by IG Lead	Peter J Streatfield		03/01/2023	IT Application / forwarded to IT and IG.
1.8	20/01/23	Minor formatting changes, clarification of text in Section 7.	Peter J Streatfield	FA	20/01/2023	IT Application / forwarded to IT and IG.
Next review due	March 2023	Review - by IG lead				

Table of Contents

1.	Introduction.....	4
2.	Request Assessment Process.....	5
3.	Working From Abroad Risk Assessment Form.....	6
4.	Guidance for Managers	7
5.	Taking your device abroad	7
6.	Related employment considerations:.....	8
a.	Managing Performance	8
b.	Annual leave.....	8
c.	HMRC and tax implications	8
7.	Green List.....	9
	Appendix A – Working from Abroad - Related considerations & FAQs.....	11

1. Introduction

This procedure is part of the BC7 Remote Working Procedure.

Working Remotely from Abroad

This procedure sets out for managers the process to follow if a member of your team makes a request to work from abroad. This should be used on an exception only basis.

The aim of this process is to identify and minimise the Data Protection and Security Risks to your service area and the Council, including data breaches or a compromised network (i.e., cyber security breach). The risk of such breaches is increasing, and breaches have the potential to significantly impact organisations. Caution should be demonstrated in assessing any such requests.

Employees should be clear that the option of working from abroad is not an entitlement or to be used as additional holiday. Usual hours of work will be expected and a prompt return when the emergency subsides.

Depending on the circumstances, we have agreed to permit employees to work from abroad for a reasonable period if:

- it is an emergency of family circumstances or similar
- they can fulfil all duties remotely
- they accept liability for any additional fees and/or incidents related to the travel
- they return to work in LBR Council offices/the UK, as soon as possible and/or for a specific period agreed by the service.

This guidance only applies to assessment for green listed countries. Countries outside of this are deemed to be red list countries and such requests to work from any of these should NOT be agreed to. The assessment is on this basis, with no exceptions.

Process

Factors that require consideration include:

- Time Zone differences
- Patterns of Work
- Role-based requirements
- Accessibility needs
- Duration of employment
- Support Costs
- IT remote support limitations

Managers are asked to assess these considerations, fill in the assessment form, and read the information in the FAQs when making their decision.

It is also important that a record is kept by the manager of the decision taken *and* IT services informed to ensure they are aware of who is working abroad with IT access. It is imperative that their device is compliant and up to date with the latest build and security features. More information can be found below.

Each application will be considered individually, taking into consideration the reasons for the request. Please ensure you follow the guidance closely. ***Please note that advice & guidance is subject to change and individual circumstances may be different.***

2. Request Assessment Process

The response to the assessment of the facts and circumstances, also HR, data protection, and cyber security questions determine whether a request should be granted.

The request should be made directly to the manager and discussed between the manager and employee to ensure all facts are considered. The manager should forward the request to the Operational Director who will decide whether the request should be agreed to.

Please use the following criteria to determine whether to approve the request:

- Is it a limited period working from abroad?
- Is it a hard to fill role that would face recruitment difficulties if the employee had to leave the post to travel abroad?
- Is the length of time requested going to cause detrimental impact on service delivery if the employee is unable to be physically present?
- Is the employee willing to return to LBR if unable to work abroad?
- Will there be a condition to return to work in LBR for a set period during the travel to reduce the impact on service delivery?
- Is the employee aware of all the liabilities and their personal responsibilities should the request be granted?
- Does the risk assessment flag too many issues without any mitigation?

3. Working From Abroad Risk Assessment Form

An editable Word version of the Risk Assessment Form, which must be completed and submitted as an attachment in your Service Desk ticket, can be found here:

[Working From Abroad Risk Assessment Form](#)

Once the manager has completed the form and gained agreement from the Operational Director, keep a copy for your records and provide a copy for the IT Service Desk. It is the employee's responsibility to respond to any requests from IT with actions that will ensure the equipment/process are fit for purpose before they travel.

You must use this link to access the form and submit your request:

[Request to work abroad - Home \(service-now.com\)](#)

A request must be completed EACH time a person travels.

The IT Service Desk will acknowledge the decision and, subject to the individual requirements, will make relevant changes to operational checks to ensure the individual can continue to access Redbridge networks from the destination country. The IT Service Desk will flag any configuration or operational issues.

These could include:

- The individual's computer account is due to expire during or near dates of travel.
- The individual's device is not suitable for travel.

4. Guidance for Managers

Considerations for working from abroad requests.

Time Zone differences	Would the difference in time zones have an impact on working with other colleagues?
Patterns of Work	Are there existing patterns of work or arrangements that could not be adapted for working in the destination country?
Role-based requirements	Would working in the destination country prevent any duties being carried out by the individual?
Support needs	Are there any support needs that could not be met by working in the destination country?
Duration of employment	Is the staff member's employment due to end close to the period of travel and likely to impact transition or handover activities?
Support Costs	Are there support costs that need to be met? Is finance in place?
Insurance	LBR does not insure devices.
IT Support	Be aware that IT support will be limited to those working abroad. Broken or lost devices cannot be supported or replaced.

If you need further advice and guidance on the above, please contact your HR Business Partner and/or IT Business Partner.

5. Taking your device abroad

Managers should plan what happens operationally with the employee if their own device or LBR device is lost or stolen or has a technical issue. Please note, IT does not insure LBR devices, and does not have the facility to support people abroad. IT are unable to send replacement laptops abroad.

Employees **must** notify their line manager immediately if the IT device is lost or stolen. It is the manager's responsibility to notify IT immediately to ensure the device is disabled.

6. Related employment considerations:

a. Managing Performance

Managers should continue to monitor performance regularly even if the employee is working from abroad. As an organisation, we do not measure performance by presenteeism so managers should focus on outcomes and trust.

- E.g., is the employee making a positive impact on their job, their team, and the organisation overall even if they are not physically present?
- Communicate with your employee and agree a set of principles to help manage performance based on the SMART outcomes.

Managers should regularly check in with the employee to identify whether the working arrangement is having an impact on the delivery of pieces of work.

Managers should use the Council's performance management procedure if this begins to have a detrimental impact on service delivery. Please note, the Council's usual people management procedures will still apply to employees working from abroad.

b. Annual leave

Employees should use annual leave when planning trips abroad for leisure purposes or general travel. Working from abroad should not be used to take a 'normal' holiday. Your health and wellbeing is important and if visiting family abroad we encourage everyone to plan to use annual leave wherever possible.

Please note that should staff be unable to work when they reach their destination they should inform their manager, at the earliest opportunity, take any outstanding annual leave as paid days leave and any days beyond this will generally be taken as unpaid leave, in agreement with their manager.

Managers must amend the iTrent record regarding any paid or unpaid leave or other changes to working patterns, terms, or conditions, to facilitate any adjustments with Payroll.

c. HMRC and tax implications

Employees should not need to pay local taxes for working abroad in most countries if the stay is shorter than 183 days in a rolling 12-month period. The EU, EEA and Switzerland allow UK employees to continue to pay into UK national insurance and pensions. In other countries where no agreement exists, the UK employer must continue to deduct employee UK NICs and pay employer NICs for the first 52 weeks. Employees are responsible for clarifying additional local tax/social security requirements for the specific country they want to travel to.

FAQs – Please see Appendix A

7. Green List

Countries deemed relatively safe are based on an adequacy decision which recognises that another country provides an equivalent level of protection for personal data as the UK. A list of adequate countries is accessible from the ICO website <https://ico.org.uk>.

Please note that the list of green countries below may be subject to change in accordance with changes in adequacy.

EU	EEA	Other
Austria	Iceland	Andorra
Belgium	Liechtenstein	Argentina
Bulgaria	Norway	Canada
Croatia	Switzerland	Faroe Islands
Republic of Cyprus		Guernsey
Czech Republic		Isle of Man
Denmark		Jersey
Estonia		New Zealand
Finland		Japan
France		Israel
Germany		Uruguay
Greece		
Hungary		
Ireland		
Italy		
Latvia		
Lithuania		
Luxembourg		
Malta		
Netherlands		
Poland		
Portugal		
Romania		
Slovakia		
Slovenia		
Spain		
Sweden		

Considerations for adding countries to the Green List:

- Does the destination country have restrictive laws or policies on use of encryption that protects Council information?

Countries highlighted by Global Partners Digital's World Map of Encryption

Laws and policies¹ are assessed as having widespread restrictions that put Council Information and Individuals at risk. Working from these countries can only be approved by Information Asset Owners (IAOs) in conjunction with the Senior Information Risk Officer (SIRO).

- Are there restrictions about where information is accessed or processed from?

There may be legislative, regulatory, or statutory requirements that prevent data from being accessed outside of the UK, e.g., Department for Work and Pensions data.

Managers should know what Information the staff member has access to and should confirm with relevant Information Asset Manager(s) (IAM) if there are any restrictions on accessing data from abroad.

- Are there UK Adequacy regulations in place for the destination country?

Following the UK's withdrawal from the EU on 31 December 2020, the UK makes its own adequacy decisions about where Data can be transferred to². These adequacy decisions are indicative that the destination country takes an equivalent stance to protecting data and are therefore a good indicator that there is a low level of risk working in them.

¹ <https://www.gp-digital.org/world-map-of-encryption/>

² <https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-dataprotection-regulation-gdpr/international-transfers-after-uk-exit/>

Appendix A – Working from Abroad - Related considerations & FAQs

Q1: How can an employee request to work remotely from abroad?

A1: If you want to request working remotely from abroad, you need to complete the Working from Abroad Risk Assessment so any potential issues or impact can be considered before reaching an outcome. The completed form should be sent to the line manager for a decision in conjunction with the Head of Service.

It must be a request to:

- work only in a green list country
- access to a secure Wi-Fi – and not in cafes or public Wi-Fi areas.
- that the LBR device has the latest build and security features installed PRIOR to travel.

An accepted working from abroad request is subject to regular review where it may be decided that in practice, it is not feasible to support the request due to issues experienced that impact the employee or service delivery. In these circumstances, employees must agree to return to the UK immediately or take a period of annual or unpaid leave to cover the remainder of the trip. For more information, please see Q3 & Q5.

Q2: What criteria should managers consider when deciding whether to accept a working remotely from abroad request?

A2: We recognise that due to Covid-19, employees have been unable to travel abroad for a period such as, to visit family or care for a family member. As part of our commitment to being a family friendly employer, managers should be flexible and consider whether the employee would still be able to complete duties effectively whilst working in another country.

The key factors to be taken into consideration are set out in this procedure and the risk assessment form.

- Please note, staff who require access to DWP data as part of their role are not permitted to access this information from outside the UK.

Q3: What happens if employees are not able to work when they reach their destination abroad?

A3: If employees are not able to work due to network connectivity issues or imposed travel restrictions in the country, they will need to agree to take a period of annual or unpaid leave to cover the duration of the stay. Managers and employees should have a contingency plan in place if a working from abroad request is accepted. The following factors should be considered:

- The employee may experience slow internet connectivity due to the country's available download speed.
- The employee may cause accidental damage to their device (IT Services are unable to ship equipment abroad).
- The employee may need to agree time back if they experience periodic system failures e.g., 'downtime' throughout the agreed working hours.
- The potential cyber security threat which could mean the employee is temporarily blocked from accessing to our network from abroad.
- The working from abroad arrangement may need to end if work is impacted on day-day basis. This should be discussed with your manager meeting on a weekly basis and depending on the circumstances, the employee may be required to return to the UK as soon as possible (within 24 hours) or take a period of annual or unpaid leave. While the employee arranges to return, this could mean a period of no cover for the service.

Q4: What happens if the employee experiences IT issues whilst working from abroad?

A4: For regular IT Support, employees should follow the same procedures as in the UK:

IT support is available between 8am–6pm Monday to Friday (excluding Public Holidays).
+44 20 8708 4455.

Preferred method of reporting or requesting support:

- [Create Support Ticket - Home \(service-now.com\)](https://service-now.com)
- Password Self-service reset: <https://passwordreset.microsoftonline.com/>

Theft or loss of device:

Employees **must** notify their line manager immediately if the IT device is lost or stolen. It is the manager's responsibility to notify IT immediately to ensure the device is disabled.

You must also complete the Data Breach/Security Incident form:

- [Data Breach/Security Incident](#)

Q5: What liabilities will the employee need to accept if their working from abroad request is granted?

A5: The employee will accept liability and not hold the Council responsible for the following:

- arranging adequate travel insurance cover which must include working abroad as LBR Personal Liability is UK based only
- paying for flights or additional fees related to travel when unexpected circumstances arise, and you are required to return to work in the UK
- ensuring passport validity and the correct visa is obtained ahead of the trip
- complying with applicable public health guidance (e.g., quarantine periods) both in the host country and on return to the UK
- accepting liability for any incidents that occur in the host country
- ensuring personal safety, working from the host country at own risk
- accepting that their employment contract remains subject to UK law and jurisdiction whilst working in a different country (salary will only be paid into a UK bank account and will be subject to relevant payroll deductions).
- maintaining all the usual precautions to working safely remotely, e.g., following the IT Code of Conduct, data protection guidelines
- accepting that they will need to use annual/unpaid leave or return to the UK immediately if their manager deems the working from abroad arrangements as unsuccessful
- making additional tax and social security declarations, if required

Employees should not need to pay local taxes for working abroad in most countries if the stay is shorter than 183 days in a rolling 12-month period. The EU, EEA and Switzerland allow UK employees to continue to pay into UK national insurance and pensions. In other countries where no agreement exists, the UK employer must continue to deduct employee UK NICs and pay employer NICs for the first 52 weeks. Employees are responsible for clarifying additional local tax/social security requirements for the specific country they want to travel to.

Q6: I have agreed a working from abroad request subject to review, how do I manage this and my team member?

A6: Along with considering all the above, managers should think about whether the request to work from abroad can be managed across the team for the proposed duration. Managers should hold review meetings every week to assess whether the arrangement is working in practice and consider the following:

Core hours/ collaborative hours – agree hours that employees must be contactable with flexibility around time zones. Employees should prepare to work evenings to ensure they are able to respond within a reasonable UK timeframe if they plan to travel further away.

Ground rules – with any flexible working arrangement, agree general day-to-day expectations to ensure there is minimal service disruption.

Health and safety – discuss whether the employee has an adequate workstation set up, as well as making sure they feel mentally and emotionally well throughout their stay.

Check ins – be flexible about team meetings and 121s, this could mean moving them earlier/later in the day/week so the employee can join in from overseas.

Liability – ensure employees are aware that they will need to seek their own advice on host country requirements and accept that they are working from abroad at their own risk.

Q7: What happens if the employee becomes unwell whilst abroad?

A7: If you become too unwell to work during your travel, you must follow the usual Sickness Absence Management Procedure to notify and inform your manager of the reason and how long you expect to be absent from work.

If you are still unwell at the end of the agreed travel period, you will need to provide a 'fit note' covering your absence from the 8th calendar day, signed by a doctor stating what is wrong with you to receive sick leave. You should return to the UK as soon as you are well enough to do so.

In circumstances where you are required to self-isolate abroad even if you are no longer sick, the service will need to identify whether it is possible to continue working from abroad during the period of isolation or agree an extended period of unpaid/annual leave to cover the absence. It is the employee's responsibility to arrange a flight back to the UK as soon as possible.

Q8: What additional requirements are in place for dealing with employees on existing Tier 2 General/Skilled Worker Visas when agreeing overseas working?

A8: Employees on Tier 2 General/Skilled Workers Visas can work overseas if agreed by management. Any agreement will need to be reported to UK Visas and Immigration (ULVI) through the Sponsorship Management System. Please contact your HR Business Partner prior to its commencement. LBR will be required to adhere to the same statutory reporting requirements for these employees as would be applicable were they working within the UK. Many, if not most of these reporting requirements are covered in the policy as set out above, particularly those relating to satisfactory performance of duties, as this is the essential criteria that the employee is satisfying the visa requirements.

It should be noted that UKVI can review any Tier 2 General/Skilled Worker Visa arrangement at any time to ensure compliance with immigration legislation. Managers will need to ensure that they are monitoring any agreed overseas working arrangements continuously and advise HR immediately if they believe there has been a breach of compliance.

Employees on Tier 2 General/Skilled Worker Visas should be aware that any time spent outside the UK may have a detrimental impact on future applications for settlement in the UK. It is the responsibility of the employee to familiarise themselves with the Home Office requirements in this regard as Settlement Applications are related to the person, and not the role they undertake within LBR.

LBR/December 2022