Procedure

Working from Abroad

1. Introduction

This policy is applicable to Council employees and provides the necessary framework to apply to work from abroad for an agreed short-term period of time. It is not intended to facilitate employees being permanently based in another country or to take/extend a 'normal' holiday, employees should use annual leave.

The Council is committed to agile working and there may be circumstances where it is an option/appropriate to work from abroad. This is a complex area and employees who wish to propose that they spend a period of time working from abroad should discuss this with their manager at the earliest opportunity and follow the procedure set out in this document. There is no right to work from abroad and managers will need to consider carefully whether any such request can be accommodated without impacting service delivery. There are other important considerations the manager must take into account, including for example, access to the Council's IT Network.

The Risk Assessment (See Appendix A) must be completed by the employee and will be carefully reviewed by the manager to inform the decision on whether to agree the employee's request.

2. Eligibility

Not all roles can be undertaken remotely and so it may not be possible to accommodate working from abroad requests due to the nature of the employee's job role. However, depending upon the outputs required and other factors, employees may work from abroad for a defined period so long as:

- The application is for a defined period of no more than 3 months.
- The employee follows the correct application procedure and their application is approved in advance.
- Applications should not be made retrospectively.
- The employee's role can be performed from a remote, overseas location.
- The employee understands that their contract of employment continues to be governed solely by English law and that the employee is liable for any and all tax and other similar costs they incur as a result of working abroad.
- The employee must be able to fulfil all their duties, to the required standard, remotely.
- Arrangements put in place, agreed and recorded with their manager are adhered to.
- The employee returns to their place of work when required and accepts all liability for additional fees and incidents relating to their travel.

3. Responsibilities

Managers:

- Familiarise yourself with the Working from Abroad Procedure and Information Assurance guidance note
- Ensure staff can fulfil duties while working from abroad
- Ensure applications have gone through the appropriate approval process
- Regularly review working arrangements where applications are approved

Staff:

- Familiarise yourself with the Working from Abroad Procedure and Information Assurance guidance note
- Follow the correct application and approval process in advance of travel
- Can fulfil duties while working from abroad
- Maintain regular contact with Manager, immediately notifying them of any issues affecting your ability to work
- Be prepared to return to the UK if a reasonable request to do so is made by the Council

HR&OD:

- Responsible for keeping the policy and procedure up to date and
- Providing advice to staff and managers

4. Application Process

Employees must have completed their probationary period before an application can be granted.

Employees who would like to request working remotely from abroad will be required to submit a request in writing clearly stating why the application is being made, for how long, the arrangements they will make to ensure duties are carried out etc., and complete the Working from Abroad Risk Assessment so that any potential risks, issues and impact can be considered. The application and completed form should be sent to their line manager and Director who will reach a decision to approve the request or not. Applications cannot be made retrospectively.

Once the line manager has answered all questions satisfactorily and access can be approved in line with the policy, the following details only should be sent to the Cyber Security Team Cyber-Security@onesource.co.uk:

- Employee name
- Destination country
- Dates of working from abroad period.

The application form should be sent to people.establishment@onesource.co.uk to be placed on the employee's personal file.

5. Essential Criteria

The following essential criteria must be met or the request will be denied:

- The employee's role does not require direct access to systems that hold personal data owned by partner organisations, for example NHS, Metropolitan Police, DWP, as access to those is only possible from within the UK.
- The employee does not work in a role that requires them to be physically present or available during core or specified hours.
- The employee must be prepared to return to the UK if a reasonable request to do so is made by the Council.

6. Additional Factors

Managers are required to assess and agree the individual risk assessment and will consider a series of additional factors when deciding whether to accept the request. Also refer to Working from Abroad IT Guidance (insert link).

Factor	Potential Issues and Solutions
Role	Can the role be carried out to required standards from the proposed location?
Length of time	Is this reasonable? Does it pose a potential detriment to service delivery?
Risk assessment	Risks to individuals and data must be identified and the actions proposed to mitigate them recorded.
Outcomes	The means by which a colleague will keep in regular contact with their manager and teams should be set out in detail. The employee cannot plan to miss regular meetings and 'catch – up' later.
Working hours covered	Covering team activities, attendance at meetings, time zone differences.
Use of sensitive data	Data protection issues.
Destination, environment	Negative impact on employee's health affecting ability to carry out work.
Emergency contact details	Unable to reach employee. Ensure details are updated in Fusion.
IT / Network	Unable to access suitable network. Issues of coverage and accessibility. Equipment issues.

7. Further Information

- Requests to work from abroad permanently will not be granted.
- Authority to work from abroad for a defined period is not a right.
- Salaries will only be paid as though the employee was in the UK with all relevant deductions made and into an account deemed suitable by the Head of People Transactional Services.

- Requests cannot run consecutively.
- All agreed requests are subject to regular review.
- Managers and employees will agree core hours and day to day availability expectations to ensure there is no service disruption.
- Employees must carry out their duties as normal including virtual attendance at team meetings, one to ones etc.
- Employees may face unexpected issues when they reach their destination abroad, for example network connectivity or travel restrictions. It is the employee's responsibility to have a contingency plan in place. Employees will need to agree a period of annual or unpaid leave to cover the duration of the stay if such issues cannot be resolved.
- If an employee becomes unwell while abroad they must follow the Sickness Absence Management Procedure and inform their manager. However, this will not usually result in the authorised period being extended.
- All arrangements in the submitted Risk Assessment as agreed must be adhered to.
- If it is apparent that the arrangements in place are not sufficient and performance is being affected, or if role requirements have changed and there is a requirement to attend the office in person, the arrangements (which are subject to a weekly review) can be cancelled by the Council at its discretion.
- Arrangements made must be recorded.

8. Senior Information Risk Owner Exceptions

There may be circumstances when Information Governance and Security considerations lead to a request being denied. Should the Head of Service decide that, based on business need, the request should be granted, an application for an exception must be made to the SIRO (Senior Information Risk Owner) via the DPO (Data Protection Officer). The SIRO's decision will be final.

9. Cyber Security and Data Protection Considerations

Working from abroad presents compliance issues under data protection and technical security compliance. If you have been approved to work from abroad, accessing your services must be performed via one of the recommended approaches, see link below.

Use a personal device to connect to your remote desktop service located here.

Taking a corporate device abroad is not recommended as it may contain information that should reside within the UK. Using a VPN is not recommended and may be disconnected by the security team if used from another country to protect the Council's systems. The full technical note is found here (insert link).

Effective date	Review date	Owner	Approved by
		HR&OD	