Solent
NHS Trust

Overseas Workers / Working Policy

Solent NHS Trust policies can only be considered to be valid and up-to-date if viewed on the intranet. Please visit the intranet for the latest version.

Purpose of Agreement	The policy has been implemented to advise both staff and managers of the processes and approval criteria that must be followed before a member of staff can work overseas. Additionally, the policy outlines the technical and security requirements that must be followed, to safeguard the Trust and its data, whilst working overseas.
Document Type	Policy
Linked to O-SOP	Overseas Workers / Working Data Protection & Cyber Security (Network Access) O-SOP
Reference Number	Solent NHST/Policy/IG26
Version	V1
Name of Approving Committees/Groups	ICT Group, Information & Cyber Security Group, Digital Workforce Group, Digital Information Group, Policy Steering Group, Clinical Executive Group, Staff Networking Group
Operational Date	July 2023
Document Review Date	July 2025
Document Sponsor (Job Title)	Senior Information Risk Owner
Document Manager (Job Title)	Data Protection Officer, Head of Information Governance and Security
Document developed in consultation with	Information & Cyber Security Group ICT contractors Staff Networking Groups Equality and Diversity Groups
Intranet Location	Business Zone>Policies
Website Location	FOI Publication Scheme
Keywords (for website/intranet uploading)	Overseas Working, Overseas Workers, Working abroad

Review and amendment log

Version Number	Review date	Amendment section no.	Page	Amendment made / summary	Changes approved by

SUMMARY OF POLICY

This policy outlines the criteria and approval process for staff wishing to work overseas and/or managers which to appoint staff to work overseas. The policy is written to support both managers and staff in undertaking appropriate assessments to consider if it is viable for staff to work overseas. As well as outlining the approval processes that must be undertaken before overseas workers / working can be implemented.

1. **Approval Criteria (outlines in Section 3):**

   Overseas Worker: Services wishing to appoint to or amend an existing staff position to an overseas worker, must ensure that one of the following criteria has been met;

   - Where a position is determined 'hard to fill' through unsuccessful recruitment and the role being listed on the national skills shortage list
   - Where a position is determined 'hard to fill' through more than one round of unsuccessful recruitment
   - Where the role can be carried out remotely, without detriment to service and patient safety

   Overseas Working: Adhoc requests to work overseas, will only be considered, whereby one of the following criteria has been met;

   - If a member of staff is conducting business overseas, on behalf of the Trust and requires access to the network
   - If a member of staff is overseas, under personal circumstances, but it is vital (impact upon business) that they have access to the Trust's network and/or work whilst overseas.

2. **Requests for working overseas on a permanent or adhoc basis (outline in Section 3 and Appendix B, C & D):** Staff / managers must complete and submit approval applications, for any overseas working, which must go through the approval process, before overseas working can be formally authorised.

3. **Approval Process (outlines in Section 4 – 7 and Appendix A):** Regardless if a request is for the appointment (or contract amendment) of an overseas worker or a request for overseas working, staff and managers **must be aware** that there are several levels of approval that must be met, in order to permit working overseas; **all** approval processes **must be** approved, before overseas working can be permitted.

   - Initial approval to confirm that an employee has met the criteria for overseas workers / working
   - Employment Law criteria's have been met (for overseas workers only)
   - Cyber Security Assessment has determined that there are no or low risks to working within the country requested
   - Overseas laws and requirements, to facilitate working within their country can and have been met.

4. **Cyber Security Assessments (outlines in Section 4 – 7 and Appendix A):** Cyber security assessments are part of the approval process but will also be conducted weekly. If a cyber security threat level changes, approval to work overseas can be revoked and if the cyber security threat level is deemed high, access can be revoked with immediate effect.

Table of Contents

Overseas Workers / Overseas Working Policy

1. INTRODUCTION & PURPOSE

1.1. Solent NHS Trust as part of its agile working and to support recruitment have approved the option of allowing staff to work from overseas, under certain circumstances.

1.2. This policy outlines the circumstances in which staff will be approved for working overseas, as well as the requirements, assessments and approvals that would need to be undertaken.

1.3. This policy outlines the circumstances in which staff will **not** be approved for working overseas.

1.4. This policy has been written to support both staff and managers when considering a request for an employee to work overseas.

1.5. This policy has been written to ensure that whilst supporting overseas working, that the Trust continues to meet its legal obligations around Employment Law and Data Protection Legislation (inclusive of ensuring that data remains secure at all time and cyber security requirements are met)

2. SCOPE & DEFINITIONS

2.1. This policy applies to locum, permanent, and fixed term contract employees (including apprentices) who hold a contract of employment or engagement with the Trust, and secondees (including students), volunteers (including Associate Hospital Managers and Patient Safety Partners), bank staff, Non-Executive Directors and those undertaking research working within Solent NHS Trust, in line with Solent NHS Trust's Equality, Diversity and Human Rights Policy. It also applies to external contractors, agency workers, and other workers who are assigned to Solent NHS Trust.

2.2. **Overseas Worker:** This is a worker that has been employed or their contracted amended, with the knowledge of supporting both frequent overseas working and long periods of overseas working.

2.3. **Overseas Working:** Is a term that is used to support adhoc requests to work overseas, whereby there is not a long-term expectation from either the staff member or manager, that this will be a long-term arrangement and therefore no contractual changes are required.

3. CRITERIA FOR OVERSEAS WORKERS / WORKING

3.1. **Overseas Worker:** Services wishing to appoint to or amend an existing staff position to an overseas worker, must ensure that one of the following criteria has been met;

- Where a position is determined 'hard to fill' through unsuccessful recruitment and the role being listed on the national skills shortage list
- Where a position is determined 'hard to fill' through more than one round of unsuccessful recruitment
- Where the role can be carried out remotely, without detriment to service and patient safety

3.2. **Overseas Working:** Adhoc requests to work overseas, will only be considered, whereby one of the following criteria has been met;

- If a member of staff is conducting business overseas, on behalf of the Trust and requires access to the network

- If a member of staff is overseas, under personal circumstances, but it is vital (impact upon business) that they have access to the Trust's network and/or work whilst overseas.

Requests for overseas working should be submitted to the Senior Information Risk Owner (SIRO), via the Information Governance Team InformationGovernanceTeam@solent.nhs.uk. The SIRO will review the request against the criteria outlined in Section 3 of this policy.

4. APPROVAL PROCESS FOR OVERSEAS WORKERS / WORKING

4.1. Appendix A outlines the process that staff and managers must go through, to assess, approve and implement (where applicable) the ability to work overseas, whether this be for an adhoc purpose or a change in employment location.

4.2. **Recruiting to an Overseas Workers Position:** Manager wishing to request to appoint staff to an overseas worker's position must complete Appendix B and submit their request to their Operations Director, and then Head of People Partnering & OD, for approval.

4.3. **Staff Request for Overseas Worker / Working:** Staff wishing to request to work overseas, must either complete Appendix C – Overseas Workers Request (change of contract will be required) or Appendix D – Overseas Working (Adhoc Requests).

4.4. **Approval Process:** Appendix D, identifies a flow diagram which outlines the approval routes that must be taken, before a request ***from a staff member***, for overseas worker / working can finally be approved.

4.5. **Approval Process:** Regardless if a request is for the appointment (or contract amendment) of an overseas worker or a request for overseas working, staff and managers **must be aware** that there are several levels of approval that must be met, to permit working overseas; **all** approval processes **must be** approved before overseas working can be permitted.

- Initial approval to confirm that an employee has met the criteria for overseas workers / working
- Employment Law criteria's have been met (for overseas workers only)
- Cyber Security Assessment has determined that there are no or low risks to working within the country requested
- Overseas laws and requirements, to facilitate working within their country can and have been met.

4.6. **Requests that maybe declined:** Staff and managers are to be aware that requests for working overseas, although will be considered, are not guaranteed to be approved. Requests maybe declined if they;

- Don't meet the criteria for overseas workers / working
- Employment law requirements cannot be met
- The country that the employee wishes to work from, has been identified a cyber security threat (this can also include a Country's refusal to allow encrypted devices such as laptops, encrypted communication, or remote VPN (Virtual Private Network) access)
- It is not possible to meet the requirements, outlined by the country that the employee wishes to work from, in order to facilitate access

4.7. **Time Period:** Regardless if a request is for the appointment (or contract amendment) of an overseas worker or a request for overseas working, staff and managers **must be aware** that due to the complexity of the assessments required to ensure that the Trust meets its legal and mandatory requirements, a period of 6 weeks' notice is required.

- Requests will be processed as soon as possible, but within a 3-month period

- Contracts for overseas workers (or contract changes) should not be issued, until all approval criteria / assessments have been completed
- Requests for overseas working, due to the very nature they are adhoc, can often occur in cases of emergency and therefore with short notice. In these cases, best endeavours will be undertaken by the relevant departments to support the request but cannot be guaranteed. Therefore, requests for overseas working should be submitted ASAP.

5. PEOPLE SERVICES OPERATIONAL REQUIREMENTS

5.1. **Employment Law & implications assessment:** Before any staff member can work overseas, an Employment Law & implications assessment must be undertaken to ensure that the legal requirements of every country an employee has requested to work from, have been assessed and can be adhered to. Legal advice may need to be sought by the Head of People to be assured of any risk.

5.2. **Pre-employment checks and Professional Body Registration:** These remain the same as all staff employment. Please refer to the recruitment policy and/or your registration body for more details.

5.3. **Contractual Requirements:** The Trust must have in place, specific contracts for staff working overseas. The contract is to include requirements to ensure that majority of work is conducted within the UK and an agreement and awareness that overseas working is subject to an initial employment law and cyber security assessment, that will be periodically reviewed and that the ability to work overseas could be terminated if it is no longer feasible from a business / clinical safety perspective and / or if the cyber security threat level changes (immediate revocation without notice could be enacted as a result of cyber threat alerts issued by the National Cyber Security Centre (NCSC)). This also includes reasons relating to an individual's performance and/or conduct.

5.4. **Training:** Staff approved to work overseas will still be required to undertake induction and mandatory training. Managers must make arrangements for an Induction to take place, ideally onsite (if not possible, this will be reviewed on a case-by-case basis, between the manager and People Services), and work with IT colleagues to ensure safe receipt/delivery of IT equipment; completion of statutory & mandatory training, support line manager with onboarding programme into to team and service, assess any on-call requirements with line manager

5.5. **Expenses:** Staff expenses to facilitate overseas working are not the responsibility of the Trust, with the employee remaining responsible for these, except for exceptional circumstances. However, expenses may be covered for the induction period only, including hotel accommodation which must be booked through the Trust Travel Desk. These expenses are to be agreed beforehand and service lines are to cover any accommodation costs for overseas workers where applicable.

6. DIGITAL SERVICES OPERATIONAL REQUIREMENTS

6.1. The member of staff who will be working overseas, needs to be in the UK at the time of enabling this access in order for the setup process to be completed successfully and to ensure equipment is in working order.

6.2. Requests need to be submitted at least six weeks before travelling in order to allow for internal governance and technical setup processes to be completed.

6.3. The equipment that can be allocated to overseas workers, can consist of (where there is a business need);

- Laptop
- Keyboard
- Mouse
- Screen
- Smartcard
- Mobile phone

6.4. The security assessment of a specific country will consider all necessary factors in order to be compliant with Trust and national policies. These will include, but limited to:

- Use of VPN
- Use of telecommunications equipment
- Use of encryption

Countries must allow all the above to be utilised if an employee was to work abroad.

6.5. Staff working overseas will be able to access support from the Trust's ICT Service Desk during its operational hours – Monday – Friday, 07:00 – 19:00 GMT / BST

6.6. If a Trust owned device is lost or compromised overseas it should be reported immediately as per process identified in the IT Security Policy

6.7. Trust devices must be connected to VPN in order to receive security patches and updates

6.8. Trust mobile phones can be remotely wiped. Trust laptops cannot currently be remotely wiped.

6.9. The cost to enable someone for overseas working will be added to the Digital catalogue as a standard request with associated charge. Ongoing costs directly attributed to overseas working e.g., mobile data roaming costs will be recharged back to service lines.

6.10. Assets are to be managed in line with standard Solent Asset management practices

7. DATA PROTECTION & CYBER SECURITY OPERATIONAL REQUIREMENTS

7.1. Before any staff member can work overseas, a cyber security assessment of the country the staff member is wanting to work within, must be undertaken.

7.2. The cyber security assessment will assess the cyber security threat level (utilising the National Cyber Security Centres cyber assessment) for the intended country and any cyber security actions / activities that must be undertaken, in order to legally facilitate working with the intended country.

7.3. The cyber security assessment will be undertaken by the Trust's Cyber Security Manager. The assessment will then be reviewed and approved or rejected, by either the Trust's Data Protection Officer (Cyber security Lead).

7.4. The assessment will conclude if the intended country is deemed as.

Rating	***Comments***
Green Rating – Overseas working will be approved	Country has been deemed to have no or low cyber security threat and no other action is required in order to work within the country.
Amber Rating – Overseas working is subject to additional assessment, actions, and approval, before overseas working can be approved.	Country has been deemed to have no, low or medium security threat, however further action is required in order to work within the country (whereby the intended country of working legally requires activity, restrictions, registration, etc… to be undertaken, before working within the country commences). Additionally, if the country has been identified as medium security threat, a risk assessment will need to be undertaken and reviewed and approved by the Trust's SIRO.
Red Rating – Overseas working will not be approved	Country has been deemed to have a high security threat and / or does not allow the use of VPN and / or encrypted devices within the country.

7.5. The Trust must undertake continual (monthly) cyber security assessments of all countries, where staff are working overseas; these will be conducted by the Trust's Cyber Security Manager and monitored through the Information & Cyber Security Group. Cyber Security assessments and therefore overseas working approval are not a one-off activity and if the cyber security threat level changes to medium or high, approval can be revoked, in some cases revoked and removed with immediate effect (in cases of high security threat level).

7.6. It is important for staff to be aware that if their cyber security assessments identifies that the country, they intend to work from has been identified as an Amber Rating, and additional activities are required to meet legal requirements within the country they wish to work, that these activities may need to be undertaken by the staff member themselves and not the Trust. Staff will be made aware of any actions they are required to undertaken and what evidence of competition is required (as this will differ from case to case). Access and approval to work abroad will not be granted, nor facilitated until these actions have been completed. Evidence of competition will be held by the Information Governance & Digital Security Team. Staff should also be aware that in some cases it may not be possible to meet the legal requirements of the intended country, and this will be outside of the control of the Trust – the request will therefore need to be declined.

7.7. When working overseas, access to the network must be undertaken via the utilisation of VPN access. This is to provide a secure and encrypted linked to the Trust's network. Access outside of VPN will only be authorised by exception and to a limited number of cloud-based applications. Authorised will be undertaken through alternative secure connections and Multi-Factor Authentication. *Please refer to the Trust's Overseas Workers / Working Data Protection & Cyber Security Standard Operating Procedure.*

7.8. The Trust's *Overseas Workers / Working Data Protection & Cyber Security Standard Operating Procedure* outlines the operational steps that will be undertaking in order to implement and support overseas working securely and how cyber security threat levels will be assessed and monitored.

8. ROLES & RESPONSIBILITIES

8.1. **Staff:**

- Are responsible for completing the appropriate initial request form Appendix C – Overseas Workers Request or Appendix D – Overseas Working (Adhoc Requests).
- Discussing the request with their manager
- Understand that approval is subject to a number of assessments and approval processes
- Must not plan to work overseas, until all approvals have been granted
- Understand that requests will only be approved, when all of the relevant approval assessments have been met
- Understand that they may be required to undertake certain activities themselves, in order to support requests, where the cyber security assessment returns an "Amber Rating"
- Understand that access can be revoked (in some cases without notice), should the countries cyber threat level increase
- Seek independent financial and income tax advice prior to submitting their request
- Must ensure that they always log on via VPN to access the network and that they must log on as a minimum of once a week (if not actively working), to ensure that their account remains live
- Must ensure that they notify the ICT and IG Team of the travel arrangements, travel dates and country of destination.
- Must ensure that they notify the ICT and IG Teams, if their travel dates change at any point e.g., return to the UK sooner or later, so that the appropriate security adjustments can be made.
- Are responsible for the costs of returning equipment on end of contract/employment

8.2. **Managers:**

- Managers should ensure that before approving overseas workers and / or overseas working, that business needs have been assessed and the impact on the business if staff member is unable to work and patient safety should patient consultations be impacted by a staff member unable to connect to the Trust's network.
- Managers should ensure that business continuity plans, and contractual arrangements are in place, in the event of the following actions
  - VPN access is unavailable
  - Staff member temporarily loses access to Wi-Fi
  - Cyber security threat level changes and overseas working approval is revoked
- Managers must plan for an Induction to take place, ideally onsite, and work with IT colleagues to ensure safe receipt/delivery of IT equipment; if this is not possible discussions must be had with both the ICT, IG and HR Teams, to ensure that safe and appropriate alternative arrangements can be made.
- Completion of statutory & mandatory training, support line manager with onboarding programme into to team and service, assess any on-call requirements with line manager

- Manager must plan to ensure that Clinical supervision and management supervision can still be maintained, when working overseas, prior to overseas arrangements being approved.

8.3. **People Services:**

- People Services will provide advice around employment law, jurisdiction, risks of working overseas and precedent
- Will liaise with external legal counsel for specific advice
- Will administer all approved requests

8.4. **Cyber Security Manager**

- Are required to undertake the Cyber Security Assessment
- To provide a monthly report to the Information & Cyber Security Group of all staff working overseas and the current cyber security threat level and any "risky logins" alerts associated with the staff member's account.
- To ensure that security changes are reverted back to standard security settings, at the end of the agreed period of overseas authorisation
- Assess the cyber security risk associated with this policy and advise both the Trust's Data Protection Officer and SIRO of any increased risks
- Make recommendations to the Trust's Data Protection Officer and SIRO, should a countries cyber security threat level increase.
- To monitor the cyber security threat level of any country overseas, whereby a staff member is authorised to work from
-

8.5. **Data Protection Officer**

- To review and approve cyber security assessments
- To assess any the cyber security risks identified and/or recommendations made by the Trust's Cyber Security Manager and undertake risk assessments to present to the Trust's SIRO for decision
- To undertake the initial review of Overseas Working (adhoc) requests, to ensure that they meet the criteria for consideration, before submitting to the SIRO for approval.

8.6. **SIRO**

- To assess any the cyber security risks identified and/or recommendations made by the Trust's Cyber Security Manager and/or Data Protection and make appropriate decisions.
- To review of Overseas Working (adhoc) requests, to ensure that they meet the criteria for consideration, and undertake an approval decision.

9. TRAINING

9.1. All Trust staff will be made aware of their responsibilities regards completing Induction Training and Mandatory Training

9.2. Staff working overseas must complete Data Protection and cyber security training, through their annual Information Governance Training, prior to working overseas.

9.3. Compliance with this training requirement will be monitored by the Learning & Development Team.

10. EQUALITY IMPACT ASSESSMENT

10.1. A thorough and systematic assessment of this policy has been undertaken in accordance with the Trust's Policy on Equality and Human Rights.

10.2. The assessment found that the implementation of and compliance with this policy has no impact on any Trust employee on the grounds of age, disability, gender, race, faith, or sexual orientation. See Appendix E

11. SUCCESS CRITERIA / MONITORING EFFECTIVENESS

11.1. Unauthorised access overseas: Overseas access is monitored by both the Trust's outsourced ICT Contracts and the Cyber Security Manager. Connection overseas will be cross referenced against authorised overseas workers / working requests and if the staff member is not on the approved list, the staff members account will be blocked and reported to the Trust's Cyber Security Manager to investigate.

11.2. Authorised access overseas: monthly reports will be provided to the Information & Cyber Security Group of all staff working overseas and the current cyber security threat level and any "risky logins" alerts associated with the staff member's account.

Weekly monitoring will be undertaken for any country overseas, whereby a staff member has

12. REVIEW

12.1. This document may be reviewed at any time at the request of either staff side or management but will automatically be reviewed 3 years from initial approval and thereafter on a triennial basis unless organisational changes, legislation, guidance, or non-compliance prompt an earlier review.

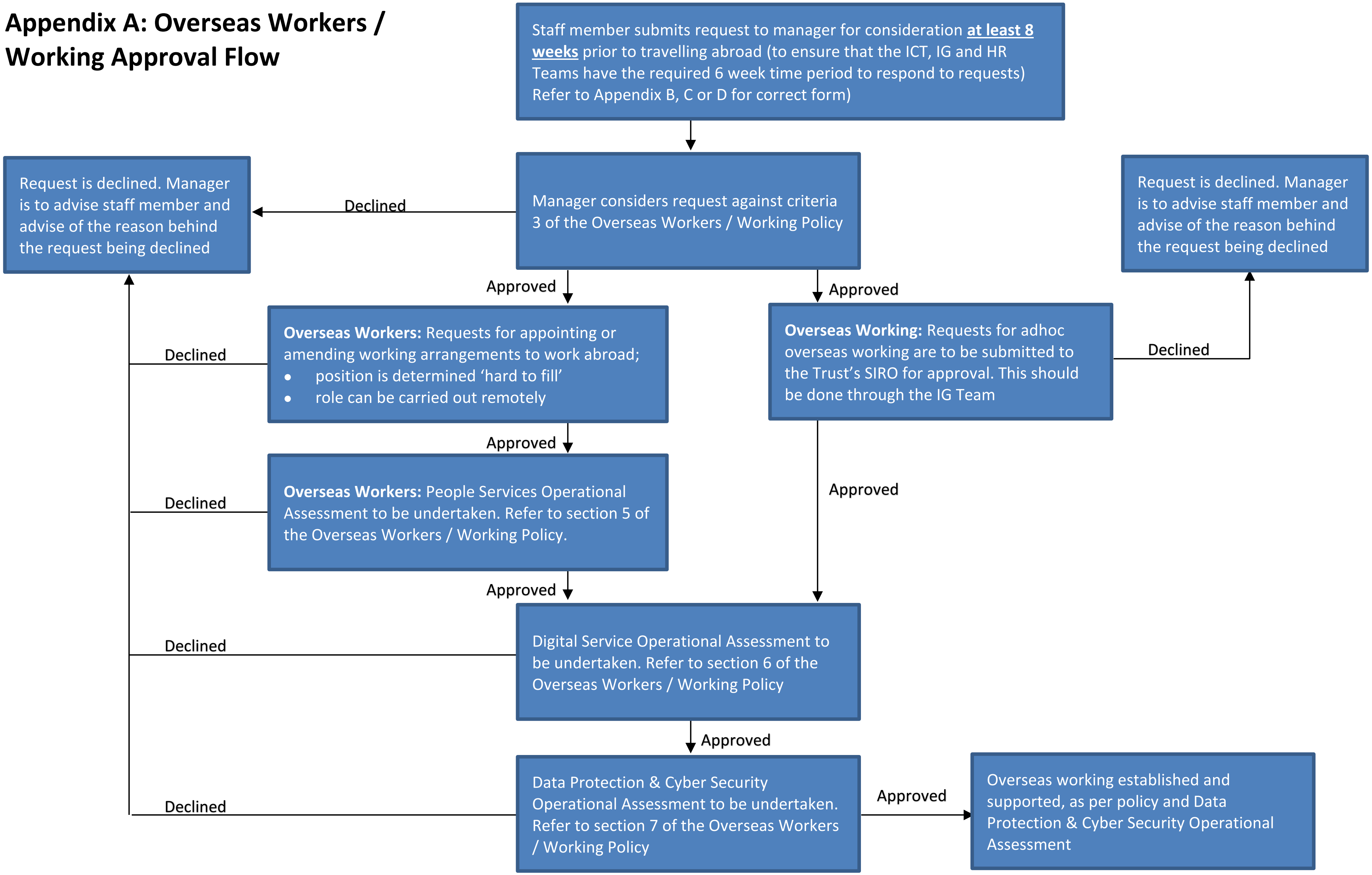
13. REFERENCES AND LINKS TO OTHER DOCUMENTS

- Data Protection & Compliance Policy
- Overseas Workers / Working Data Protection & Cyber Security Standard Operating Procedure
- Recruitment and Selection Policy
- Pre-employment Checks Standard Operating Procedure
- Agile Working Standard Operating Procedure
- Performance Management Policy
- IT Security Policy
- Mobile Working Policy
- Management of Mobile Devices Policy

14. GLOSSARY

Abbreviation:	Meaning
SIRO	Senior Information Risk Owner
VPN	Virtual Private Network

Appendix A: Overseas Workers / Working Approval Flow



Staff member submits request to manager for consideration **at least 8 weeks** prior to travelling abroad (to ensure that the ICT, IG and HR Teams have the required 6 week time period to respond to requests) Refer to Appendix B, C or D for correct form)

Manager considers request against criteria 3 of the Overseas Workers / Working Policy

Request is declined. Manager is to advise staff member and advise of the reason behind the request being declined

Overseas Workers: Requests for appointing or amending working arrangements to work abroad;

- position is determined 'hard to fill'
- role can be carried out remotely

Overseas Working: Requests for adhoc overseas working are to be submitted to the Trust's SIRO for approval. This should be done through the IG Team

Request is declined. Manager is to advise staff member and advise of the reason behind the request being declined

Overseas Workers: People Services Operational Assessment to be undertaken. Refer to section 5 of the Overseas Workers / Working Policy.

Digital Service Operational Assessment to be undertaken. Refer to section 6 of the Overseas Workers / Working Policy

Data Protection & Cyber Security Operational Assessment to be undertaken. Refer to section 7 of the Overseas Workers / Working Policy

Overseas working established and supported, as per policy and Data Protection & Cyber Security Operational Assessment

Appendix B: Overseas Workers Recruitment Application Form

Section 1 – to be completed by Manager

RECRUITMENT FOR OVERSEAS WORKING REQUEST FORM			
Vacancy Details			
Post Title		**Vacancies** (quantity)	
Service Line		**Is this linked to a risk on the risk register?** (risk number)	
Manager Name		**Is the post hard to fill?** (please attach evidence)	
Role Site / Location / Base		**How many times have you attempted to fill post?** (please attach evidence)	
Country (if known)		**Is this a current vacancy, or is the person occupying the role moving?**	

Business case for overseas working
Brief Description of the role (key deliverables an accountabilities) (attach JD)
Why is it necessary to recruit and permit overseas working for this role?
Please note additional knowledge, skills, qualifications and/or experience for the post
What impact could this have on the existing team/roles?
What are the intended contractual arrangements? (temp or perm, is the person mainly UK based, or mainly overseas based? Will they be an employee of the Trust or a self-employed consultant?)

Authorisation		
Operations Director		
Name:	Signature:	Date:
Head of People Partnering & Organisational Development		
Name:	Signature:	Date:
Senior Information Risk Owner (On behalf of Executive Team)		
Name:	Name:	Name:

Section 2 – to be completed by People Services – Employment Law and other Considerations

Country under consideration:	[state country]
Consideration	Outcome
People Partnering	
What is the Contractual Status of the role due to be? (PAYE employee, contractor etc)	
What will the worker status be? (i.e., employee/worker)	
Where will the worker be resident (UK or other country)?	
Will the worker return to the UK and if so, how often and for how long approx.?	
Host country employment rights vs. resident country employment rights (the rights will be in line with the country they will mainly reside in) – what considerations do we need to make and what might we need to be aware of?	
Does this align with the Workforce Plan and People Strategy? Is this within budget?	
Resourcing and Attraction	
Is a visa / residency required to be applied for?	
Training – what training or assessment (if any) will the individual need to undertake to be able to practice?	
How long will induction and onboarding take? (Speak to the Head of People Partner or Deputy People Partner to ensure this fits with Workforce Plan)	
Pay and Reward	
Tax implications (mainly income tax)	
Is the worker able to claim full UK tax relief on earnings? (see gov.uk website)	
Payroll – is the tax viable, working with HMRC?	
Information Governance	
IG Requirements – does the resident country have encryption restrictions?	

Appendix C: Overseas Workers Request Application Form

Section 1 – to be completed by Manager

CHANGE TO OVERSEAS WORKING REQUEST FORM	
Vacancy Details	
Post Title	
Service Line	
Manager Name	
Role Site / Location / Base	
Country (if known)	

Business case for overseas working
Brief Description of the role
Why is it necessary to permit overseas working?
Please note additional knowledge, skills, qualifications and/or experience for the post
What impact could this have on the existing team/roles?
What country will the employee wish to work from?
What equipment will the employee need to work abroad?
What are the intended contractual arrangements? (temp or perm, is the person mainly UK based, or mainly overseas based? Will they be an employee of the Trust or a self-employed consultant?)

Authorisation		
Operations Director		
Signature:	Signature:	Signature:
Head of People Partnering & Organisational Development		
Signature:	Signature:	Signature:
Senior Information Risk Owner (On behalf of Executive Team)		
Name:	Name:	Name:

Resourcing Team (Contract Issued)		
Name:	Signature:	Date:
Salary Point:	Band:	Starting Band:
Resourcing Team (Actioned on ESR)		
Name:	Signatures:	Date:

Section 2 – to be completed by People Services – Employment Law and other Considerations

Country under consideration:	[state country]
Consideration	Outcome
People Partnering	
What is the Contractual Status of the role due to be? (PAYE employee, contractor etc)	
What will the worker status be? (i.e., employee/worker)	
Where will the worker be resident (UK or other country)?	
Will the worker return to the UK and if so, how often and for how long approx.?	
Host country employment rights vs. resident country employment rights (the rights will be in line with the country they will mainly reside in) – what considerations do we need to make and what might we need to be aware of?	
Does this align with the Workforce Plan and People Strategy? Is this within budget?	
Resourcing and Attraction	
Is a visa / residency required to be applied for?	
Training – what training or assessment (if any) will the individual need to undertake to be able to practice?	
How long will induction and onboarding take? (Speak to the Head of People Partner or Deputy People Partner to ensure this fits with Workforce Plan)	
Pay and Reward	
Tax implications (mainly income tax)	
Is the worker able to claim full UK tax relief on earnings? (see gov.uk website)	
Payroll – is the tax viable, working with HMRC?	
Information Governance	
IG Requirements – does the resident country have encryption restrictions?	

Appendix D: Overseas Working (Adhoc) Request Application Form

ADHOC OVERSEAS WORKING REQUEST FORM			
Post Title		Employee Name	
Service Line		Assignment Number	
Manager Name			

Business case for overseas working
Has the staff member requesting to work overseas met the requirement of adhoc overseas working, as defined by Section 3.2 of the Overseas Workers & Working Policy?
☐ Member of staff is conducting business overseas, on behalf of the Trust and requires access to the network ☐ Member of staff is overseas, under personal circumstances, but it is vital (impact upon business) that they have access to the Trust's network and/or work whilst overseas.
Please provide supporting information as to how the staff member meets the above criteria.
When is the staff member travelling and when is their return date?
What country will the employee wish to work from?

Authorisation		
Service Manager		
Name:	Signature:	Date:
Data Protection Officer		
Name:	Signature:	Date:
Senior Information Risk Owner (SIRO)		
Name:	Name:	Name:

Appendix E: Equality Impact Assessment

Step 1: Scoping and Identifying the Aims

Service Line / Department	Information Governance	
Title of Change:	Overseas Workers / Working Policy	
What are you completing this EIA for? (Please select):	Policy	*(If other please specify here)*
What are the main aims / objectives of the changes	The policy has been implemented to advise of the processes and approval criteria that must be followed before a member of staff can work overseas.	

Step 2: Assessing the Impact

Please use the drop-down feature to detail any positive or negative impacts of this document /policy on patients in the drop-down box below. If there is no impact, please select "not applicable":

Protected Characteristic	Positive Impact(s)	Negative Impact(s)	Not applicable	Action to address negative impact: *(e.g. adjustment to the policy)*
Sex			X	
Gender reassignment			X	
Disability			X	
Age			X	
Sexual Orientation			X	
Pregnancy and maternity			X	
Marriage and civil partnership			X	
Religion or belief			X	
Race			X	

If you answer yes to any of the following, you MUST complete the evidence column explaining what information you have considered which has led you to reach this decision.

Assessment Questions	Yes / No	Please document evidence / any mitigations
In consideration of your document development, did you consult with others, for example, external organisations, service users, carers, or other voluntary sector groups?)	Yes	Staff networking groups
Have you taken into consideration any regulations, professional standards?	Yes	Data Protection Legislation Gender Recognition Act

Step 3: Review, Risk and Action Plans

How would you rate the overall level of impact / risk to the organisation if no action taken?	Low	Medium	High
	■	□	□
What action needs to be taken to reduce or eliminate the negative impact?	N/A		
Who will be responsible for monitoring and regular review of the document / policy?	Data Protection Officer		

Step 4: Authorisation and sign off

I am satisfied that all available evidence has been accurately assessed for any potential impact on patients and groups with protected characteristics in the scope of this project / change / policy / procedure / practice / activity. Mitigation, where appropriate has been identified and dealt with accordingly.

Equality Assessor:	*Sadie Bell, Head of IG & Digital Security*	*Date:*	*27/06/2023*