Working Overseas

Policy and Procedure

1 Introduction

1.1 Working overseas is generally not supported at Oxford City Council. However this policy sets out the process that allows individuals to work overseas in a safe and responsible way.

1.2 This policy is not intended to facilitate employees being permanently based in another country or to take/extend a 'normal' holiday.

1.3 Any exceptional agreement to overseas working will be considered on a case by case and short-term basis and must have prior approval of the Head of People, the Director of Law, Governance and Strategy, and the Deputy Chief Executive City and Citizens' Services.

2 Who this policy covers

2.1 This policy covers all Oxford City Council employees, workers, members and volunteers.

2.2 It applies to contractors, consultants, agency workers, self-employed individuals directly accessing council data to complete work for the organisation.

3 What this policy covers

3.1 This policy includes any work-related activity conducted on any device whilst overseas (outside of the United Kingdom).

3.2 It includes but is not limited to the checking and composition of emails, attending meetings, speaking to colleagues or completion of written work.

3.3 Equipment used overseas includes laptops, tablets, smartphones, and any other devices that can store or access council data. Council applications and data include emails, documents, databases, and any other information that belongs to the council or is processed by the council.

4 Working overseas

4.1 Employees should not access any work systems or emails whilst overseas without permission, and to do so could raise security risks and have serious legal implications.

4.2 Employees should not take any council devices outside of the UK unless they have raised a request to work overseas, and it has been approved.

4.3 In line with the ICT Remote Access to Networks and Equipment Policy employees should not install or use any unapproved software or private VPNs to council equipment.

4.4 Employees should not use personal devices to access the council network, including Microsoft 365, whilst working overseas.

4.5 Failure to obtain approval to carry out any work-related activity when abroad could result in disciplinary action.

5 What are the risks?

5.1 Working overseas carries a number of risks to individuals and the organisation.

Data Security

5.2 Where a role involves the use or processing of personal data, this could give rise to data protection issues, including a potential breach of data protection laws and a higher risk of a cyber-attack.

5.3 The level of risk is dependent on the following factors:

- The sensitivity of the data and nature of the work
- The systems accessible by the user
- The data protection law in the destination country
- Any political and or security concerns regarding the destination country.
- The duration of the requested stay

5.4 Employees who have access to DWP data will not be permitted to work abroad unless their access to all DWP data is removed prior to leaving the UK.

5.5 Employees who process data on behalf of a third-party organisation may need to seek that organisation's approval prior to processing any such data abroad.

Tax

5.6 If duties are carried out in a different country, subject to protection under a taxation agreement, the other country may seek to tax the income individuals receive for those duties.

5.7 Even with short-term work overseas, there may be additional reporting obligations in the overseas country.

Right to Work

5.8 There may be immigration restrictions on working in another country, even for a limited period. Permission may be required in advance of travel unless the individual is a national of that country.

5.9 There could also be an impact for any non-British/ Irish nationals, as any absence may impact their settled status, visa, or their eligibility to apply for other types of status in the future.

Employment protections

5.10 If employees live and work abroad, even for short periods, they can become subject to the jurisdiction of that country. This could include minimum rates of pay, paid annual holidays and rights on termination.

Health and Safety

5.11 In the UK employers have a duty to protect the health, safety and welfare of their employees. Different countries have different rules, so any work must meet these varying obligations.

5.12 Consideration must also be given to additional threats at the time of any request such as crime, extreme climate, infectious diseases, political unrest, natural disasters and terrorism.

Contractual agreements

5.13 Employees may not be able to carry out work overseas where their role involves contractual agreements. Current legislation does not allow for employees to enter into or negotiate contracts overseas as this may be viewed as forming a "permanent establishment" in another country.

6 When will a request to work overseas be accepted?

6.1 Requests to work will be considered on a case-by-case basis and accepted only in exceptional circumstances.

6.2 Requests to work will be accepted strictly on the following basis:

- The employee's role can be effectively performed remotely and carried out lawfully from the country in question.
- The employee is not in probation, notice period, performance improvement or disciplinary proceedings.
- The period spent working overseas will not be more than 90 days in a rolling 180-day period.
- A risk assessment is completed that sets out the specific risks and mitigations that will be put in place (see appendix 1).
- The employee has obtained and proven their right to work in the overseas country.
- The employee will accept liability for any costs incurred as a result of working overseas including travel, accommodation, insurance and legal compliance.
- The employee will accept liability for any costs incurred to the Information Commissioner as stated in Data Protection Law should a data breach occur due to the employee's failure to comply with this policy.
- Work related activity will be carried out using only council equipment (no personal devices) with the strict use of a council approved VPN when accessing the council network and any work-relation information, including Microsoft 365.
- The employee will not use council devices for personal use whilst abroad
- Access to the council network will be via a private connection. Connection to public Wi-Fi is not permitted under any circumstances.

- All work will be password protected in case equipment is lost or stolen.
- The employee will use a strong unique password and two factor authentication.
- Written approval is obtained by the Director of Law, Governance and Strategy, Head of People and Deputy Chief Executive City and Citizens' Services.
- The council reserves the right to withdraw the agreement at any time, with reasonable notice.
- If, for any reason access to work systems, facilities or permissions is revoked or restricted, the employee will need to return to the UK in order to resume duties.

6.4 Under no circumstances will individuals be permitted to work from any of the listed countries, where there are data ed:

- Afghanistan
- Belarus
- China
- Haiti
- Iran
- Lebanon
- Libya
- North Korea
- Russia
- South Korea
- South Sudan
- Syria
- United States of America
- Yemen

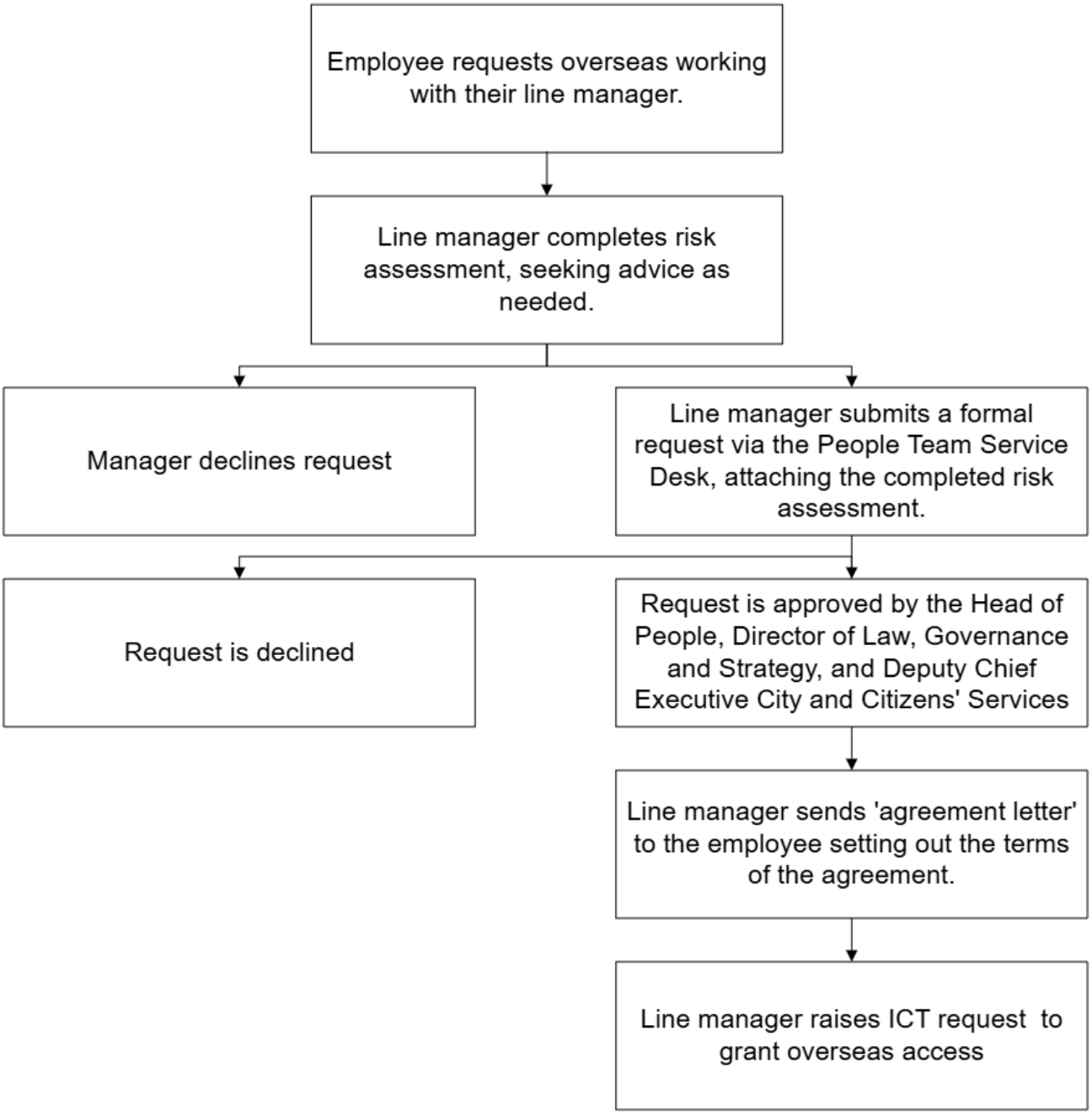
These are countries considered to have 'high-risk conditions' based on information from the UK Foreign Office and the European Commission adequacy decision as to whether a country offers an adequate level of data protection.

6.5 Permission to work abroad cannot be assumed because it was approved in the past. Each request should be treated as a separate application.

6.6 Failure to meet any of these requirements could result in disciplinary action being taken.

7 Procedure

7.1 This flowchart sets out the procedure that must be followed:



Risk Assessment

7.2 The risk assessment should be completed by the line manager, seeking advice as needed from the People, ICT, and Data Protection teams.

7.3 The employee raising the request is responsible for obtaining and paying for any additional specialist advice required e.g. tax, contractual or employment obligations.

Agreement letter

7.4 If a request is approved by the Head of People, Director of Law, Governance and Strategy and Deputy Chief Executive City and Citizens' Services, a notification will be sent to the ICT team to ensure data security provisions can be put in place.

7.5 Upon approval, written agreement must be sent to the employee by the line manager, setting out the terms of the arrangement. A member of the People Consultancy Team must review the Agreement Letter before it is sent.

7.6 While the detail of the Agreement Letter will depend on the circumstances typical provisions include:

- The agreed dates of working overseas.
- The agreed working hours and exact location.
- Expectations around meeting performance standards and responsibilities of the role.
- Confirmation that the employee will be liable for any additional income taxes or employee social security which may be charged because of their decision to work for a period in an overseas location (with the employer being authorised to make additional deductions or seek reimbursements, if necessary, for this purpose).
- Confirmation that the employee will be responsible for any personal tax declarations or social security contributions that need to be made.
- Confirmation that the employee will be responsible for any Council equipment they use overseas and must have sufficient insurance to cover the replacement of any equipment if it is lost, damaged or rendered unusable.
- Requirement for the employee to provide proof of the legal right to work in the destination country for the agreed period.
- Confirmation that the employee will bear the full cost of flights, accommodation, medical insurance, and any other costs related to working abroad.
- Requirement for any phishing attempts, lost devices or suspected problems to be reported immediately.
- Confirmation that if the employee becomes ill while being abroad, they must follow the Attendance Management Policy, and any sick notes obtained must be officially translated into English.
- Confirmation that if they are unable to work whilst overseas for any reason, the remaining time overseas can be taken annual leave or special unpaid leave.
- Statement that confirms the council reserves the right to withdraw, suspend or amend the agreement at any time.

8 Procedure for Members

8.1 Whilst members are not subject to the same request procedure when planning to work overseas, they must still meet the following criteria:

- A risk assessment is completed that sets out the specific risks and mitigations that will be put in place (see appendix 2).
- The member will accept liability for any costs incurred to the Information Commissioner as stated in Data Protection Law should a data breach occur due to the member's failure to comply with this policy.

- Work related activity will be carried out using only council equipment (no personal devices) with the strict use of a council approved VPN when accessing the council network and any work-relation information, including Microsoft 365.
- The member will not use council devices for personal use whilst abroad
- Access to the council network will be via a private connection. Connection to public Wi-Fi is not permitted under any circumstances.
- The employee will use a strong unique password and two factor authentication.
- Approval is obtained by the Director of Law, Governance and Strategy and Deputy Chief Executive City and Citizens' Services.

8.2 A risk assessment must be completed and reviewed by the DPO (Director of Law, Governance and Strategy) and SIRO (Deputy Chief Executive City and Citizens' Services) in advance so that any risks can be identified and mitigations put in place. Completed risk assessments should be sent to Committee and Member Services for processing.

8.3 Upon agreement, ICT must be notified and an Agreement Letter sent to set out the terms of the arrangement.

8.4 Failure to do this may result in access to all OCC systems being withdrawn immediately until the member's return to the UK.

9 Monitoring and review

9.1 This policy will be regularly reviewed in consultation with trade unions.

10 Appendix 1 – Working Overseas Risk Assessment Form for Employees/ Workers

Section 1: Employee/ member details			
Name		Service Area	
Job Title		Employment Type	
Country they wish to work from		Requested dates (from – to)	
Address when working abroad			
Section 2: Detail of the request			
What is the reason for the request? *If the request is not accepted – what is the impact on the organisation?* *How will it impact the person's ability to do their job? Consider working hours, collaboration, in person meetings. Would any adjustments need to be made?* *What is the current Foreign Office travel guidance to this country? Consider crime, climate, public health information, political unrest, natural disasters and terrorism.* *What is the work environment like? Consider privacy, connectivity, equipment.* *Does the employee have proof of the right to work in the requested location?* *What are the GDPR rules in the requested location? For information on a Countries adequacy status please check this site: Data protection adequacy for non-EU countries.* *What data will the employee access whilst working overseas? Is any of it personal or sensitive data? What systems does the employee have access to?*			

As part of their working environment, how will they keep data secure and protect the confidentiality of any data or work conversations they may have? *As part of the employee's role are they involved in contract negotiation or agreement at all?*

Section 3: Consideration of risks and mitigations				
Risk	**Likelihood**	**Impact**	**Mitigating Action**	**Owner**
What is the risk?	*How likely is it to happen? (Unlikely – likely)*	*Consider the impact on the person, team, organisation and customers*	*What actions can be taken to reduce the likelihood of this risk occurring?*	*Who is responsible for completing the mitigating action?*
Inability to carry out the tasks required of the role	[Unlikely / likely]	[Low / medium / high]		Line Manager
Additional health and safety obligations in the overseas country	[Unlikely / likely]	[Low / medium / high]		Health and Safety Team
Additional tax obligations to the overseas country	[Unlikely / likely]	[Low / medium / high]		Line Manager
No right to work in the overseas country	[Unlikely / likely]	[Low / medium / high]		People Team
Additional employment rights in the overseas country	[Unlikely / likely]	[Low / medium / high]		People Team
Additional GDPR obligations in the overseas country	[Unlikely / likely]	[Low / medium / high]		Data Protection Team
Sensitivity of data accessible	[Unlikely / likely]	[Low / medium / high]		Data Protection Team

Restrictions on ability to make contractual agreements on behalf of the Council	[Unlikely / likely]	[Low / medium / high]		Legal Services
Loss or damage of Council equipment	[Unlikely / likely]	[Low / medium / high]		ICT
Breach of OCC systems	[Unlikely / likely]	[Low / medium / high]		ICT
Breach of DWP data sharing regulations	[Unlikely / likely]	[Low / medium / high]		ICT
Add any other risks specific to this post.				

11 Appendix 2 - Working Overseas Risk Assessment Form for Members

Section 1: Employee/ member details			
Name		Requested dates (from – to)	
Country they wish to work from		Address when working abroad	
Section 2: Detail of the request			
What is the current Foreign Office travel guidance to this country? Consider crime, climate, public health information, political unrest, natural disasters and terrorism. *What are the GDPR rules in the requested location? For information on a Countries adequacy status please check this site: Data protection adequacy for non-EU countries.* *What data will the member access whilst working overseas? Is any of it personal or sensitive data? What systems does the employee have access to?* *As part of their working environment, how will they keep data secure and protect the confidentiality of any data or work conversations they may have?*			

Section 3: Consideration of risks and mitigations			
Risk	**Likelihood**	**Impact**	**Mitigating Action**
What is the risk?	*How likely is it to happen? (Unlikely – likely)*	*Consider the impact on the person, team, organisation and customers*	*What actions can be taken to reduce the likelihood of this risk occurring?*
Additional health and safety obligations in the overseas country	[Unlikely / likely]	[Low / medium / high]	
Additional GDPR obligations in the overseas country	[Unlikely / likely]	[Low / medium / high]	

Sensitivity of data accessible	[Unlikely / likely]	[Low / medium / high]	
Breach of OCC systems	[Unlikely / likely]	[Low / medium / high]	
Add any other risks specific to this post.			