www.oxford.gov.uk
OXFORD CITY COUNCIL

To:	**Council**
Date:	26th January 2026
Report of:	Gail Malkin, Head of People
Title of Report:	Working Overseas Policy and Procedure

Summary and recommendations	
Decision being taken:	Seeking agreement to implement a new policy and procedure relating to working outside of the United Kingdom.
Key decision:	No
Cabinet Member:	Councillor Nigel Chapman, Cabinet Member for Citizen Focused Services and Council Companies
Corporate Priority:	None.
Policy Framework:	Relevant policy in Policy Framework or state none.

Recommendation(s): That Council resolves to:

1. Approve the following:
    a. Working Overseas Policy and Procedure for Employees
    b. Working Overseas Procedure for Members

Information Exempt from Publication	
State in here what information is to be exempt from publication – where it is, attach it as an appendix and name the appendix as you describe It here	N/A

Appendix No.	Appendix Title	Exempt from Publication
Appendix 1	Risk Register	No
Appendix 2	Equality Impact Assessment	No
Appendix 3	Working Overseas Policy and Procedure for Employers	No
Appendix 4	Working Overseas Procedure for Members	No

Introduction and background

1. The process of requesting to work overseas is not currently documented.

2. In recent months the organisation identified a number of employees, workers and members working overseas without having notified ICT before travelling.

3. For employees in particular this poses a high risk to the council in terms of:
    - Data security
    - Tax implications
    - Right to work
    - Employment protections
    - Health and safety
    - Contractual agreements

4. Following the recent cyber incident, all access to council systems outside the UK has been stopped.
5. Access can be granted by ICT, but to mitigate the significant risks this carries, the policies provide a process that should be followed to enable working overseas in a safe and responsible way.

Update since last Council meeting

6. When this policy was considered by Council on 6th October 2025 the following points were raised:

Points raised	Response
The list of countries where access will not be granted should not include the US or South Korea.	We have removed the US and South Korea from the list of counties where access will not be granted. For employees only (not members), a request to work from the US may not be granted depending on the US State, the data protection rules in place and the type of data individuals would need access to.

The policy states that employees / members must accept liability for any costs incurred to ICO should a data breach occur. How much is this?	The Information Commissioner can issue a monetary penalty directly to individuals for their failure to comply with the Data Protection Act 2018. Individuals can also face criminal liability, where fines are then imposed by the court. There is no statutory maximum fine but in practice, fines have ranged from hundreds to a few thousand pounds, depending on severity.
Members needing to use council owned devices. Can light / portable loan devices be provided from ICT?	It is recommended that council owned devices are used, and devices can be provided by ICT. If this is not feasible, Members can use personal devices to access the Council network, and ICT recommend using a VPN to give additional protection.
Israel and Palestine not on the list of banned countries. Should they be?	The list of 'banned' countries is based only on Data Adequacy. There are other countries where travel is not advisable as guided by the Foreign Office, and access would not be approved. This would be considered as part of the risk assessment completed before travel.
Putting the restrictions in place only makes it more likely that individuals wanting to work overseas will circumvent the process by using alternative VPN to appear to come from the UK.	The reason for using a VPN is to help mitigate the increased likelihood of a data breach. The policy seeks to help individuals better understand the risks if they do not follow the process. For employees the disciplinary process would be invoked for any unapproved overseas access to the council network.

Proposed parameters to working overseas

7. We are proposing two separate policies based on the level of risk.
8. Employees and workers are likely to have access to council systems holding personal and sensitive data, where the impact should a data breach occur is a significant risk to the organisation and needs to be avoided where possible.
9. For members, access to the council network whilst travelling overseas may be required to allow them to keep in touch with residents and to continue to manage casework, primarily through emails.
10. By having a policy for employees and workers, and a separate procedure for members, we can implement steps to protect the organisation whilst meeting the needs of members and the council.

Working Overseas Policy and Procedure for Employees

Who the policy applies to:

11. This policy covers all Oxford City Council employees and workers.

What the policy covers:

12. This policy includes any work-related activity conducted on any device whilst overseas (outside of the United Kingdom). It includes but is not limited to the checking and composition of emails, attending meetings, speaking to colleagues or completion of written work.

Parameters to working overseas for employees / workers

13. Requests to work will be considered on a case-by-case basis and if the following apply:

- 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.
- 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 that as stipulated in Data Protection Law they may be personally liable for any costs incurred to the Information Commissioner should the member fail to follow this procedure and a data breach occur.
- 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-related 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 long, unique password (minimum 12-14 characters) and Multi-Factor Authentication (MFA) for all system access.
- Written approval is obtained by the DPO (Director of Law, Governance and Strategy), Head of People and SIRO (Deputy Chief Executive City and Citizens' Services). The SIRO holds the final decision on all requests. The DPO is able to veto a request where there is a justified data security risk.
- 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.

14. For employees there are a number of countries listed on the policy where working overseas will not be approved. These are countries considered to have 'high-risk conditions' based on information from the European Commission adequacy

decision as to whether a country offers an adequate level of data protection compliance.

Working Overseas Procedure for Members

Who the procedure applies to:

15. This procedure covers all Oxford City Council Members.

What the procedure covers:

16. This procedure sets out the steps members should take to notify OCC of a need to access the council network outside of the UK, allowing any risks to be identified and mitigated in advance of travel.

Parameters to working overseas for members

17. Any requests to access the council network overseas will be arranged on the following basis:

    - A risk assessment is completed so that any risks can be identified and mitigations put in place.
    - It is advised that Members will access the council network via a Council-owned device, however where not feasible Members can use a personal device with a VPN.
    - The risk assessment is reviewed by the DPO (Director of Law, Governance and Strategy) and SIRO (Deputy Chief Executive City and Citizens' Services).

18. For members there are a number of countries we advise against accessing council networks from, though any risks and mitigations will be considered on a case-by-case basis:

    - Afghanistan
    - Belarus
    - China
    - Haiti
    - Iran
    - Lebanon
    - Libya
    - North Korea
    - Russia
    - South Sudan
    - Syria
    - Yemen

Other implications

Consultation and communications

19. This policy has been reviewed and agreed by the Unions and the Council Leadership Team.

20. Upon its agreement we will share employee and member communications to clarify the position on working overseas and set out the procedure that must be followed for any future requests.

Financial implications

21. There are no financial implications. The policy is clear that any costs associated with working outside of the UK will sit with the individual, not the council.

Legal issues

22. Failure to put mitigations in place before individuals carry out council-related work overseas carry significant legal risk, which are set out in the Policy and Risk Register. This includes legal implications on both the individual if:

- Personal or sensitive data is breached.
- The individual does not have the legal right to work in that country.
- The individual becomes subject to the legal jurisdiction of the overseas country.

Level of risk

23. The risk without a robust policy and procedure in place is significant. As indicated by the Risk Register, putting in place a procedure involving a risk assessment and specific criteria the risks can be sufficiently avoided or reduced.

Equalities impact

24. A copy of the Equalities Impact Assessment is attached in Appendix 3.

Report author	Victoria Taylor
Job title	People Consultancy Manager
Service area or department	People Services
Telephone	07549410420
e-mail	vtaylor@oxford.gov.uk