Privacy Threshold Assessment

Project Details

Project name	Employee Assistance Program (EAP) portal
Business owner	Manager HR Support
Threshold assessment drafter	A/g Manager HR Support
Description of the project	Access to the LifeWorks platform, a new and improved EAP portal for all staff to access. Geoscience Australia's EAP provider, SMG Health, was acquired by LifeWorks in 2021. As a result, Geoscience Australia staff will be offered access to the LifeWorks platform. Lifeworks offers a range of additional services to those currently provided through the SMG Health portal.
Types of personal information being handled as part of the project	To enable single sign-on, the HR Support team will provide a list of all employees' names and their work email addresses to LifeWorks so that they can verify they are Geoscience Australia employees. We have a single sign-on arrangement with the existing EAP portal provided by way of the same personal information. The HR Support team will be able to remove or add employees. No other personal information other than name and work email will be provided by Geoscience Australia without seeking the consent of the employee. Staff who do not wish to access to the portal may request HR remove them from the list provided to LifeWorks. EAP reports contain aggregated data, not individual level data, so individual details and usage cannot be identified by HR or our employees. The tool provides the opportunity for individual employees to set up their own profiles (with their own personal information) to receive personalised content. An individual may choose to enter their personal information, which could include age, weight, height, family details, preferences or interests and contact details. Providing any additional personal information is at the employee's discretion. Prior to accessing services, Lifeworks will provide staff with information about their privacy rights and will seek consent to the terms and conditions applicable to LifeWorks' EAP Services. Any subsequent use and disclosure of personal information will be in accordance with the consent obtained and only to the extent reasonably necessary for LifeWorks to perform its obligations under its agreement with Geoscience Australia. Under the LifeWorks privacy policy, personal information may be stored in databases located in the United States, Canada, the United Kingdom or other countries in accordance with the laws of that jurisdiction. The USA, Canada and the UK have privacy legislation that affords

	substantially similar protections to Australian privacy legislation.
What is the purpose of handling the personal information?	The use of personal information as described above is reasonably necessary for Geoscience Australia to effectively meet its commitments to employee health and wellbeing. As an employer, Geoscience Australia has an obligation to provide a safe, professional, productive and supportive work environment. As part of our obligations under the Work Health and Safety Act and our Mental Health Strategy, Geoscience Australia has committed to providing a number of wellbeing initiatives including an Employee Assistance Program (EAP). The EAP provides individual counselling and broader wellbeing programs. The new portal provides staff with the option of accessing additional tools and personalised plans, if they choose to, aimed at enhancining their overall wellbeing.
Stakeholders	All employees and HR

Part 1: Personal information handling

Does the project involve new or changed ways of handling personal information?

☑ **Yes** Complete Part 2 of the assessment below.

☐ **No** It is not necessary to complete a privacy impact assessment (PIA).
Record the decision at Part 3 and file this assessment with the Privacy Officer.

Part 2: Determining potential for a high privacy risk

Consider the following questions and record each answer as 'yes', 'potentially' or 'no'. The purpose of these questions is to you help you screen for factors which point to the potential for a high privacy risk project. It's important to note that these questions are non-exhaustive, and you should also consider whether there are any other relevant factors that may indicate that your project is a high privacy risk project.

Will the project involve:	**Yes**	**Potentially**	**No**
A. Handling large amounts of personal information? *Consider the amount of personal information and the number of individuals that will be impacted by your project. Even if you consider that each individual will only have a small chance of suffering a negative impact, handling personal information on a large scale can increase the privacy risk associated with your project. You should also consider whether your project will result in significant increases in the volume of personal information being handled through new or existing channels.*	☐	☐	☑

Will the project involve:	Yes	Potentially	No
B. Handling sensitive personal information? *Sensitive personal information includes, but is not limited to, information about an individual's racial or ethnic origin, political opinions, religious beliefs or affiliations, criminal records, sexual preferences or practices, biometric information, health information and genetic information.* *The privacy risk associated with your project can increase if sensitive information is involved given the potential for adverse consequences for an individual, or those associated with the individual, if it is mishandled (for example, discrimination, mistreatment, humiliation or embarrassment).*	☐	☐	☑
C. Sensitivities based on the context in which the project will operate? *Consider the context and circumstances surrounding the project. Are there prior concerns over this type of handling or activity? Is the project likely to have community support? Is the handling of personal information novel in any way? What is the current state of technology in this area and has there been any previously identified security or technology flaws? Are there any current issues of public concern that you should factor in? What is the nature of your relationship with individuals that may be impacted by the project? How much control will they have over the handling of their personal information? Would they expect you to use their personal information in this way?*	☐	☐	☑
D. Handling personal information in a way that could have a significant impact on the individuals concerned? *Consider the potential consequences for the individuals concerned. For example, negative impacts on physical and mental wellbeing, reduced access to public services, discrimination, financial loss or identity theft.*	☐	☐	☑
E. Disclosing personal information outside of your entity? *Consider whether your project will involve sharing personal information with another entity, organisation or to any individuals other than the individual to whom the information relates. This might include the use of contractors or sub-contractors. Also consider whether your project will require the disclosure of personal information overseas.*	☑	☐	☐

Will the project involve:	Yes	Potentially	No
F. Handling personal information of individuals who are known to be vulnerable? *Consider whether the activity may have greater sensitivities or disproportionate impacts on vulnerable populations and certain groups of individuals. This could include children and seniors, people with impaired intellectual or physical functioning, people who are not native speakers of the local language, people with low levels of literacy or education, people from a low socio-economic background, people experiencing financial hardship, people who are Aboriginal or Torres Strait Islanders.* *An individual's circumstances, or the increased power imbalance between the individual and an entity, may mean, for example, they are unable to easily consent to, or oppose, the handling of their personal information, understand its implications, or exercise control over their personal information.*	☐	☐	☑
G. Using or disclosing personal information for profiling or behavioural predictions? *This includes valuation or scoring, profiling and predicting (including in relation to economic situation, health, personal preferences or interests, reliability or behaviour, location or movements).*	☐	☐	☑
H. Using personal information for automated decision-making? *This might include the use of artificial intelligence technologies or data analytics techniques on personal information to produce insights for policy-making or improved service delivery. It might also include using automated decision-making to make decisions that affect the rights, entitlements and opportunities of an individual.*	☐	☐	☑
I. Systematic monitoring or tracking of individuals? *For example, the introduction or enhancement of a surveillance system, the monitoring of communications, tracking an individual's geolocation or behaviour.*	☐	☐	☑
J. Collecting personal information without notification to, or consent of, the individual? *This might include collecting personal information about an individual from a third party without the individual's knowledge or consent. It might also include collecting personal information compulsorily under an existing, or proposed, legislative authority.*	☐	☐	☑
K. Data matching (linking unconnected personal information)? *For example, a new data matching program combining, comparing or matching personal information obtained from multiple sources.*	☐	☐	☑
L. Any other relevant factors that may have a significant impact on the privacy of individuals?	☐	☐	☑

Part 3: Decision & declaration

If you have answered 'Yes' or 'Potentially' to any of the questions in Part 2, a PIA should be completed. If you are uncertain as to whether you have considered all relevant risks, you are strongly encouraged to seek support from the Privacy Officer to ensure your assessment is thorough and complete. If still unsure, err on the side of caution and conduct a PIA.

Based on your answers above, is a PIA required?

☐ **Yes** Yes, there are (or potentially are) high privacy risk elements to this project.

☑ **No** No, a PIA is not necessary. The project does not carry any high privacy risks.

Whilst personal information (employee names, work email addresses) may potentially be stored in databases held overseas, the information will be protected in accordance with the laws of the relevant jurisdiction and is generally afforded substantially similar protections to those provided by Australia's privacy legislation. In the event of unauthorised use or disclosure of the information, the risk of serious harm to any individual is unlikely. Should staff elect to provide additional personal information in order to receive personalised services, appropriate notification will be provided and consent obtained for any subsequent use and disclosure of their information.

Business owner sign-off

Position	A/g Manager, HR Support	Date	8/10/2021

Privacy Officer sign-off

Position	A/g Director, Governance	Date	8/10/2021