Office of the Victorian
Information Commissioner

Phone: 1300 00 6842
Email: enquiries@ovic.vic.gov.au
PO Box 24274
Melbourne Victoria 3001

13 February 2024

Department of Education
Department of Employment and Workplace Relations

Via Online submission

Submission in response to the National Skills Passport consultation

The Office of the Victorian Information Commissioner (**OVIC**) is pleased to provide a submission in response to the National Skills Passport consultation paper (**consultation paper**).

OVIC is the primary regulator for information privacy, information security and freedom of information in Victoria, administering both the *Privacy and Data Protection Act 2014* (Vic) (**PDP Act**) and the *Freedom of Information Act 1982* (Vic). As such, I have an interest in initiatives likely to have an impact on individuals' personal information.

OVIC understands a National Skills Passport (**Passport**) could enable individuals to store, view and share their skills and qualifications across Vocational Education and Training (**VET**) and higher education through a digital system. This would enable individuals to demonstrate their skills to employers more effectively, encourage further education, upskilling, reskilling, and workforce mobility, among other things. For employers, the Passport could streamline the process for viewing and verifying credentials of a potential employee.

This submission comments on privacy and security considerations for government when designing and implementing the Passport. As the Passport is a federal initiative, any collection, use and disclosure of personal information for the Passport will need to comply with privacy obligations in the *Privacy Act 1988* (**Privacy Act**). This submission discusses Australian Privacy Principles (**APPs**) that may be relevant. OVIC would encourage government to engage closely with the Office of the Australian Information Commissioner (**OAIC**) throughout the development of the Passport, should government decide to implement it.

Privacy Impact Assessments and Security Risk Assessments

A digital tool such as the Passport should be designed with privacy and security front of mind. OVIC strongly recommends that government undertake a privacy impact assessment (**PIA**) in the early stages of the design of the Passport. A PIA will enable government to systematically assess and identify potential risks to the privacy of individuals' information and develop strategies to address those risks. Among a range of other benefits, a PIA ensures personal information is handled consistently with the Privacy Act, demonstrates government's commitment to protecting and respecting individuals' information, and can build public confidence in the Passport.

For similar reasons, OVIC also recommends conducting a security risk assessment to identify any potential risks to the security of information held in the platform and build adequate security protections into the design of the tool.

Privacy enhancing information practices

OVIC understands the Passport will, at minimum, contain information about an individual's tertiary education qualifications. The consultation paper states the Passport may be able to leverage information already being collected through existing student management systems used by VET and higher education service providers when building the Passport.[1] It will be crucial to ensure any personal information collected for the Passport is collected in compliance with the APPs, particularly APPs 3 and 5.

Among other obligations related to collection of personal information, government will need to ensure it collects only the minimum amount of information necessary for the Passport. Further, government will need to clearly define the purpose of collection as this will limit the ways in which the information can be used and disclosed.

The consultation paper states the Passport could connect to other relevant services and support personalised career advice and guidance on education, training and career pathways including information on workforce demand. Having a clearly defined purpose will minimise the risk of scope creep, where personal information collected for purposes related to the Passport is used for a range of other purposes not related to the Passport. In addition, minimising the amount of information collected for the Passport to that which is necessary minimises the risk of overcollection of information.

Security of information in the Passport

As the Passport will function as a digital ID credentialling tool, any personal information held in the platform will need to be secure. Government will need to take reasonable steps to protect the personal information from misuse, interference, loss, unauthorised access, modification, or disclosure as required by APP 4.

A number of large-scale data breaches in the last few years have not only highlighted the increased risk and occurrence of breaches with digital platforms, but also the capacity for breaches to have a considerable impact on a significant portion of the population and on the affected organisation.[2] It will

[1] Consultation paper, page 8.

[2] John Davidson, *'Latitude breach now one of the biggest in Australian History'* , Financial Review (27 March 2023) available at: https://www.afr.com/technology/latitude-breach-now-one-of-the-biggest-in-australian-history-20230327-p5cvjr ; Paul Smith, '*How the Optus breach will change corporate Australia forever*', Financial

be prudent for government to implement robust measures to minimise the risk and impact of a data breach should the platform be compromised.

Proactive measures that can be implemented include ensuring access to the information stored in the Passport is restricted to authorised persons only. The OAIC's Notifiable Data Breaches report for January – June 2023 noted that the leading cause of data breaches was malicious or criminal attack, with the majority of the attacks being cyber-incidents.[3] Access controls and other ICT security controls adopted to protect information held in the platform should be reviewed and audited regularly to ensure they are operating effectively.

Another key aspect of data security is ensuring personal information is destroyed or de-identified once it is no longer needed. Retaining personal information longer than necessary increases the risk of a data breach occurring. Consequently, there must be clear rules around how long personal information will be held in the platform and how that information will be disposed. Implementing strong security controls will help build public trust in the Passport and in government's ability to handle the public's personal information appropriately.

General comment

OVIC notes there are existing initiatives that provide similar services to the Passport. These include the Unique Student Identifier (**USI**), which is a unique reference number assigned to every VET and university student to track their learning and qualifications. There is also the government's Your Career digital platform designed be a single trusted source of careers information for individuals.[4] Government will need to consider, and explain to stakeholders, how the Passport will work alongside these existing platforms to ensure it is of benefit to stakeholders rather than duplicating existing initiatives and creating more complexity.

Conclusion

Thank you once again for the opportunity to respond to the development of a National Skills Passport.

I have no objection to the Department of Education and the Department of Employment and Workplace Relations publishing this submission without further reference to me. OVIC will also publish a copy of the submission on our website.

Review (30 September 2022) available at: https://www.afr.com/technology/how-the-optus-breach-will-change-corporate-australia-forever-20220929-p5bm1p; Richard Chirgwin, '*Medibank incurred $7.5million in direct tech costs after cyber-attack*', IT News (21 September 2023) available at: https://www.itnews.com.au/news/medibank-incurred-75-million-in-direct-tech-costs-after-cyber-attack-600477.

[3] Notifiable Data Breaches Report: January to June 2023, available here: https://www.oaic.gov.au/privacy/notifiable-data-breaches/notifiable-data-breaches-publications/notifiable-data-breaches-report-january-to-june-2023.

[4] Information on the Your Career platform is available here: https://www.yourcareer.gov.au/about-us.

If you would like to discuss this submission, please do not hesitate to contact Anita Mugo, Senior Policy Officer at anita.mugo@ovic.vic.gov.au.

Yours Sincerely

Joanne

Joanne Kummrow
Acting Information Commissioner