# Victorian Privacy Network meeting – 21 March 2024: Responses to questions from Q&A

## OVIC public statement on the use of personal information with ChatGPT – Anique Owen, Office of the Victorian Information Commissioner

1. **Has the use of Copilot been considered specifically, as most Victorian Government staff have access to various forms of it, as it stands today?**

OVIC issued a [Public Statement on the use of Microsoft 365 Copilot in the Victorian public sector](https://aus01.safelinks.protection.outlook.com/?url=https%3A%2F%2Fovic.vic.gov.au%2Fprivacy%2Fresources-for-organisations%2Fvps-use-of-microsoft-365-copilot%2F&data=05%7C02%7Cadriana.nugent%40ovic.vic.gov.au%7C9dc43903aa074333f9c108dc4c58f9be%7C7733a54ddd7b40bcbabbc0b08bfa2eff%7C0%7C0%7C638469192242390364%7CUnknown%7CTWFpbGZsb3d8eyJWIjoiMC4wLjAwMDAiLCJQIjoiV2luMzIiLCJBTiI6Ik1haWwiLCJXVCI6Mn0%3D%7C0%7C%7C%7C&sdata=Osp68W6KOZ9MEuznmGVcLpYEt8hwKUaQBm5rG00dthk%3D&reserved=0) in October 2023. This arose from awareness that from 1 November 2023 VPS organisations with an existing Microsoft E3 or E5 licence would be able to access and implement the tools within their organisation. The Public Statement sets out the minimum expectations for organisations before using Copilot, and highlights both the privacy and information security risks of its use.

1. **ChatGPT is just one of many products – what about others? Many third-party apps use a mix of genAI products, not just one.**

OVIC’s Public Statements on Microsoft 365 Copilot and ChatGPT include considerations that are applicable when using any generative artificial intelligence (**genAI**) platform as the privacy and information security risks are similar across genAI platforms.

Before implementation of any genAI platform, organisations must ensure they have taken steps to meet [OVIC’s minimum expectations](https://aus01.safelinks.protection.outlook.com/?url=https%3A%2F%2Fovic.vic.gov.au%2Fprivacy%2Fresources-for-organisations%2Fvps-use-of-microsoft-365-copilot%2F%23minimum-expectations-before-adopting-copilot&data=05%7C02%7Cadriana.nugent%40ovic.vic.gov.au%7C9dc43903aa074333f9c108dc4c58f9be%7C7733a54ddd7b40bcbabbc0b08bfa2eff%7C0%7C0%7C638469192242401752%7CUnknown%7CTWFpbGZsb3d8eyJWIjoiMC4wLjAwMDAiLCJQIjoiV2luMzIiLCJBTiI6Ik1haWwiLCJXVCI6Mn0%3D%7C0%7C%7C%7C&sdata=AARf0YDw2mkBDfCmwsw55m91Ttx%2BvK2sfa6eoEEnDro%3D&reserved=0) (as outlined in OVIC’s Public Statement on the use of Microsoft 365 Copilot in the Victorian Public Sector), and have an extensive understanding of how personal information is collected, used, disclosed, transferred and retained by that platform.

Where there is a risk that personal information held by a VPS organisation will be transferred, accessible, retained, used or disclosed by the genAI platform’s developers, third-party stakeholders or other consumers of the platform, personal information should not be input into the genAI platform. Doing so will contravene several Information Privacy Principles.

1. **Does OVIC have a learning module that can be used to launch ChatGPT awareness training for all agency staff through our LMS of choice?**

No, OVIC does not have a learning module to provide training and awareness when using ChatGPT for all agency staff.

VPS organisations using ChatGPT should have established guidelines, processes and training for staff that is specific to their operational environments and use cases.

When developing training and awareness initiatives around the use of genAI platforms, VPS organisations should at a minimum be focused on empowering staff to:

* Identify the purpose for using the genAI platform before inputting any information, including:
	+ considering whether the same outcome can be achieved without the use of a genAI platform;
	+ identifying tangible benefits of using a genAI platform for that purpose;
	+ evaluating whether the use of a genAI platform is appropriate, and likely to achieve the desired outcome; and
	+ evaluating whether the benefit for the organisation in using a genAI platform is reasonable and proportionate to the risk of harm to an individual if their personal information is input.
* Check whether a genAI platform has been authorised for use within their organisation. To do this, employees should contact their Privacy Officer and/or Information Security Unit or IT team to understand:
	+ whether the platform is appropriate for use; and
	+ whether there are certain settings or configurations they will need to implement, when they should do so; and
	+ what information should and should not be input.
* Understand the type of information that is being input into the genAI platform, including:
	+ Are employees able to identify whether the information is personal information as defined in section 3 of the *Privacy and Data Protection Act 2014*?
	+ Are employees able to carry out a risk assessment where it is public sector data, and identify and understand possible risks?
* Carry out privacy impact assessments, and security risk assessments, before implementing and using genAI platforms in all use cases to identify the privacy and information security risks in doing so, and what steps and controls should be implemented to protect personal information, and public sector data.
* Err on the side of caution and do not input personal information or public sector data if they are not certain. If an employee is unsure if they should input personal information or public sector data into a genAI tool, they should stop, and ask their Manager, Privacy Officer, Information Security Unit or IT team.
1. **The OVIC public statement on the use of personal information with ChatGPT outlines several ways in which use of ChatGPT is likely to breach the IPPs. The message is clearly 'don't put PI into ChatGPT'.**

**The next section is entitled 'What if input history and model training is disabled?', and lists ways in which the privacy risk may be mitigated. It is not clear whether OVIC is saying that, if these controls (or if additional controls, such as having an enterprise subscription in which model training is disabled at an organisational level, and additional protections are in place) are enabled, VPS organisations can use ChatGPT.**

**Can you please clarify?**

**Obviously, there will be other IPPs and privacy issues which would need to be considered when using ChatGPT, but a blanket ban on using any PI in ChatGPT seems to be very strict in comparison to other jurisdictions.**

ChatGPT, and all genAI platforms, continue to rapidly evolve to meet the needs of consumers, and address the privacy and information security risks raised by regulators across the world. OVIC acknowledges that as time passes, VPS organisations will have greater control over how genAI platforms collect, hold, use, retain and disclose personal information and that some risks may be mitigated. As the landscape changes, OVIC may provide further commentary to support VPS organisations to understand their obligations and risks.

At this time, OVIC’s Public Statement does not ‘ban’ the use of ChatGPT as a whole; instead it clearly sets out that personal information and certain types of public sector data should not be input into the platform.

This is because OVIC is aware that the predominant use of ChatGPT in the VPS is with ChatGPT 3.5 (ChatGPT’s free offering) where individual employees are using their personal accounts, or creating work-based accounts, without sufficient knowledge of how the platform works; how any personal information input is being used; or awareness of the risks in doing so. Further, OVIC is aware that VPS organisations do not have full visibility of how and when ChatGPT is being used, or what type of information is being input across their organisations.

Due to this, OVIC’s Public Statement addresses the current use of ChatGPT as it results in the greatest risk of harm to individuals, and there is the most serious impact to VPS organisations.

While some VPS organisations are exploring ChatGPT Enterprise subscriptions (and other genAI platforms where information input is not used to train the Large Language Model), this is of a small occurrence when compared to the widespread use of ChatGPT 3.5.

It should be noted that where a VPS organisation is using ChatGPT Enterprise or other Data Loss Prevention tools, VPS organisations still have obligations under all 10 of the Information Privacy Principles, including but not limited to IPP 1 – Collection, IPP 3 – Data Quality, IPP 4 – Data Security and IPP 9 – Transborder Data Flows, which cannot be nullified by ICT controls alone.

If your organisation is considering a ChatGPT Enterprise subscription, you are welcome to contact privacy@ovic.vic.gov.au for assistance in understanding the specific privacy risks relevant to your operational environment.

## Drafting modern notices of collection – Cassandra Meagher, Service Victoria

1. **OVIC takes the role to educate the VPS, but what about private sectors? Where can private sectors seek education and support?**

The Office of the Australian Information Commissioner (OAIC) has jurisdiction over the private sector’s collection and handling of personal information. Private sector organisations with an annual turnover of $3m or more are required to comply with the *Privacy Act 1988*. Visit <https://www.oaic.gov.au/> for more information or to contact the OAIC.

*Answered by OVIC*

1. **Do you regularly review existing collecting notices? What would be the common trigger?**

We regularly check collection notices and Service Victoria works with its partner agencies to do this. A common trigger to do so is when a service offering, or requirements to access it, is changing. Another is customer queries or complaints.

1. **Are you aware of third-party websites providing a service interacting with Service Victoria? They collect customer information and charge a premium on top of the licence cost.**

Yes, we are. We are working with the partner agency to help address this issue and are supportive of their request to change their legislation. If this is happening to other organisations, we would welcome other perspectives on how best to tackle this – please email Cassandra Meagher or Jack Coleman if you’d like to discuss.

1. **As scams are happening everywhere, should Service Victoria have a message on its forms or website to say that it doesn’t ask for bank account details, and that if someone receives a message with the Service Victoria logo and name, and it asks for financial details, that we should contact Service Victoria?**

Adding this information could be important in the future, especially for programs that Service Victoria facilitates which are prone to scams. To date, this has not been a significant problem therefore we aim to keep collection notices short, sharp and relevant.

1. **If we don't know who the information is going to be shared with when drafting notices of collection, do you think it's okay to use a generic response such as: “We will not release your personal information to any other person or body, unless (a) we have been authorised to do so by you, (b) it is permitted or required by law, or (c) it is appropriate or required in the performance of our functions?” What would you do in this situation?**

Point C is probably too broad to give the customer a clear understanding of how their information will be used. I would recommend waiting until the program has been designed and you understand the information flows, then write a more specific collection notice.

## PROV AI and recordkeeping policy – Justine Heazlewood, Public Record Office Victoria

1. **How long do public records have to be stored for? How do you ensure these are not accidentally fed into software products which have AI embedded in them?**

*How long do public records have to be stored for?*

There is no single answer to that question because it depends on the content of the record. Some records can and should be destroyed very quickly, others will need to be kept forever. This is usually set out in a [Retention and Disposal Authority](https://aus01.safelinks.protection.outlook.com/?url=https%3A%2F%2Fprov.vic.gov.au%2Frecordkeeping-government%2Fhow-long-should-records-be-kept%2Fretention-and-disposal-authorities-rdas&data=05%7C02%7Cadriana.nugent%40ovic.vic.gov.au%7C28632a0a6148463121cd08dc4d310107%7C7733a54ddd7b40bcbabbc0b08bfa2eff%7C0%7C0%7C638470120096119892%7CUnknown%7CTWFpbGZsb3d8eyJWIjoiMC4wLjAwMDAiLCJQIjoiV2luMzIiLCJBTiI6Ik1haWwiLCJXVCI6Mn0%3D%7C0%7C%7C%7C&sdata=mb%2BHX8%2B7YGlc5BbbUHu7SkUAVUnLLfGnPdk2EVQ1crQ%3D&reserved=0). There are many of these and some that apply across the board to most government agencies. Public records can only be lawfully disposed of under these authorities. We, of course, have a standard which sets out the principles that govern disposal: [Disposal Standard PROS 22/04](https://aus01.safelinks.protection.outlook.com/?url=https%3A%2F%2Fprov.vic.gov.au%2Frecordkeeping-government%2Fdocument-library%2Fpros-2204-disposal-standard&data=05%7C02%7Cadriana.nugent%40ovic.vic.gov.au%7C28632a0a6148463121cd08dc4d310107%7C7733a54ddd7b40bcbabbc0b08bfa2eff%7C0%7C0%7C638470120096131933%7CUnknown%7CTWFpbGZsb3d8eyJWIjoiMC4wLjAwMDAiLCJQIjoiV2luMzIiLCJBTiI6Ik1haWwiLCJXVCI6Mn0%3D%7C0%7C%7C%7C&sdata=Hl39NZbWa4fJK8bTec9dC%2BPecYiG%2FF%2FIKMBQ2PgZJN8%3D&reserved=0) and [advice](https://aus01.safelinks.protection.outlook.com/?url=https%3A%2F%2Fprov.vic.gov.au%2Frecordkeeping-government%2Fhow-long-should-records-be-kept%2Fretention-and-disposal-authorities-rdas&data=05%7C02%7Cadriana.nugent%40ovic.vic.gov.au%7C28632a0a6148463121cd08dc4d310107%7C7733a54ddd7b40bcbabbc0b08bfa2eff%7C0%7C0%7C638470120096139567%7CUnknown%7CTWFpbGZsb3d8eyJWIjoiMC4wLjAwMDAiLCJQIjoiV2luMzIiLCJBTiI6Ik1haWwiLCJXVCI6Mn0%3D%7C0%7C%7C%7C&sdata=rlJ2FA0tT6PKxxvJsRgtasy%2FqlPy1fpeIEJELllVdYc%3D&reserved=0) on our website.

Once records (which includes data and information) are no longer required for current business use, government agencies need to decide whether the records should be stored by the agency pending destruction or transfer, transferred to another agency (for example, due to a machinery of government change), transferred to PROV to be preserved as state archives, or destroyed. These are all types of ‘disposal’.

PROV collects and preserves permanent value records for many important reasons. These permanent records:

* preserve evidencing of the past decisions and actions;
* support transparency, openness and accountability in government;
* support research and re-use by providing documentary evidence for academic and research communities and the general public; and
* support individuals and communities to reconnect and preserve identity and memory and facilitate redress, recovery and reconciliation.

*How do you ensure these are not accidentally fed into software products which have AI embedded in them?*

Government agencies need to ensure that their teams are appropriately [resourced](https://aus01.safelinks.protection.outlook.com/?url=https%3A%2F%2Fprov.vic.gov.au%2Frecordkeeping-government%2Fstaff-resourcing-model&data=05%7C02%7Cadriana.nugent%40ovic.vic.gov.au%7C28632a0a6148463121cd08dc4d310107%7C7733a54ddd7b40bcbabbc0b08bfa2eff%7C0%7C0%7C638470120096147034%7CUnknown%7CTWFpbGZsb3d8eyJWIjoiMC4wLjAwMDAiLCJQIjoiV2luMzIiLCJBTiI6Ik1haWwiLCJXVCI6Mn0%3D%7C0%7C%7C%7C&sdata=AKvtEaPKkYWnOpWD52Pto%2FWyJ2yAp%2BACZJWe2ucdeTw%3D&reserved=0) and trained to lawfully dispose of public records so that there aren’t ‘honey pots’ of information sitting around exposed to accidental unintended uses. We encourage disposal as a key component of good information practice which mitigates the risk of security and privacy breaches, and reduces the information management overhead, storage costs and aids the discovery of reliable, relevant and accurate information.

Agencies should also use version control, metadata, and the principle of [Normal Administrative Practice](https://aus01.safelinks.protection.outlook.com/?url=https%3A%2F%2Fprov.vic.gov.au%2Frecordkeeping-government%2Fa-z-topics%2Fnormal-administrative-practice-nap&data=05%7C02%7Cadriana.nugent%40ovic.vic.gov.au%7C28632a0a6148463121cd08dc4d310107%7C7733a54ddd7b40bcbabbc0b08bfa2eff%7C0%7C0%7C638470120096154306%7CUnknown%7CTWFpbGZsb3d8eyJWIjoiMC4wLjAwMDAiLCJQIjoiV2luMzIiLCJBTiI6Ik1haWwiLCJXVCI6Mn0%3D%7C0%7C%7C%7C&sdata=fmdKiauGg%2BzkkpPBOjge7xKIwejZY4vpQfKEL87Bfr8%3D&reserved=0) disposal to limit discoverability of things like working documents, minor drafts, and duplicates.

1. **PROV compliance for all Victorian public entities is an important piece of work. How can organisations best improve PROV compliance without having to re-wire their entire information architecture, underlying processes & systems, meaning having to spend millions of dollars to achieve better compliance? Can AI support some of this heavy lifting?**

For cost effective solutions, I encourage government agencies to visit the PROV website and see our range of guidance, policies, standards and tools. Agencies can use our two [free online recordkeeping training modules](https://aus01.safelinks.protection.outlook.com/?url=https%3A%2F%2Fprov.vic.gov.au%2Frecordkeeping-government%2Flearning-resources-tools%2Fonline-recordkeeping-training&data=05%7C02%7Cadriana.nugent%40ovic.vic.gov.au%7C28632a0a6148463121cd08dc4d310107%7C7733a54ddd7b40bcbabbc0b08bfa2eff%7C0%7C0%7C638470120096161655%7CUnknown%7CTWFpbGZsb3d8eyJWIjoiMC4wLjAwMDAiLCJQIjoiV2luMzIiLCJBTiI6Ik1haWwiLCJXVCI6Mn0%3D%7C0%7C%7C%7C&sdata=SR8YAzBqxVoyhD5nuHzzciMrXEalwnHGCM8cjA3%2Big8%3D&reserved=0) to (re)train staff.

The PROV [Value and Risk Policy](https://aus01.safelinks.protection.outlook.com/?url=https%3A%2F%2Fprov.vic.gov.au%2Frecordkeeping-government%2Fdocument-library%2Fvalue-risk-policy&data=05%7C02%7Cadriana.nugent%40ovic.vic.gov.au%7C28632a0a6148463121cd08dc4d310107%7C7733a54ddd7b40bcbabbc0b08bfa2eff%7C0%7C0%7C638470120096169208%7CUnknown%7CTWFpbGZsb3d8eyJWIjoiMC4wLjAwMDAiLCJQIjoiV2luMzIiLCJBTiI6Ik1haWwiLCJXVCI6Mn0%3D%7C0%7C%7C%7C&sdata=VsKd3vD6JdiJ5nbsqwBA2cBdaPLxBClCmViHWRvZIzs%3D&reserved=0) enables agencies to focus resources on high value, high risk records/data/information as a priority. Once the high value high risk records compliance is at an appropriate level, resources can focus on other areas. Our free [Recordkeeping Assessment Tool (RKAT)](https://aus01.safelinks.protection.outlook.com/?url=https%3A%2F%2Fprov.vic.gov.au%2Frecordkeeping-government%2Flearning-resources-tools%2Frkat&data=05%7C02%7Cadriana.nugent%40ovic.vic.gov.au%7C28632a0a6148463121cd08dc4d310107%7C7733a54ddd7b40bcbabbc0b08bfa2eff%7C0%7C0%7C638470120096180248%7CUnknown%7CTWFpbGZsb3d8eyJWIjoiMC4wLjAwMDAiLCJQIjoiV2luMzIiLCJBTiI6Ik1haWwiLCJXVCI6Mn0%3D%7C0%7C%7C%7C&sdata=upgPK4UiqK30gQju3tSfUsn%2Bpse7SYi53bpj6zEVePo%3D&reserved=0) and [Information management maturity measurement tool (IM3)](https://aus01.safelinks.protection.outlook.com/?url=https%3A%2F%2Fprov.vic.gov.au%2Frecordkeeping-government%2Flearning-resources-tools%2Finformation-management-maturity-measurement-tool-im3&data=05%7C02%7Cadriana.nugent%40ovic.vic.gov.au%7C28632a0a6148463121cd08dc4d310107%7C7733a54ddd7b40bcbabbc0b08bfa2eff%7C0%7C0%7C638470120096187665%7CUnknown%7CTWFpbGZsb3d8eyJWIjoiMC4wLjAwMDAiLCJQIjoiV2luMzIiLCJBTiI6Ik1haWwiLCJXVCI6Mn0%3D%7C0%7C%7C%7C&sdata=bJoXqtX0r7OUvZxwfAKdu2rcAlnc2BhqHJPZIfczle8%3D&reserved=0) can be used to identify areas of improvement to target your work.

## In conversation: The privacy agenda for 2024 – Jordan Wilson-Otto, elevenM and Alex Kotova, Salinger Privacy

1. **What's the estimated timeline for the Privacy Act reform?**

The Government has signalled that it is committed to introducing legislation in 2024. A Bill to legislate at least some of the 38 ‘Agreed’ to proposals was anticipated in the first quarter of 2024, however, this has been delayed by the consultation on Doxxing. As the Doxxing consultation closed on 28 March, it’s not yet clear what this will mean for the timeframes of the Bill in 2024. The [Salinger Privacy hub](https://aus01.safelinks.protection.outlook.com/?url=https%3A%2F%2Fwww.salingerprivacy.com.au%2Fprivacy-reforms%2F&data=05%7C02%7Cadriana.nugent%40ovic.vic.gov.au%7Cc1ca139220fb431affb408dc48b8953b%7C7733a54ddd7b40bcbabbc0b08bfa2eff%7C0%7C0%7C638465204842843974%7CUnknown%7CTWFpbGZsb3d8eyJWIjoiMC4wLjAwMDAiLCJQIjoiV2luMzIiLCJBTiI6Ik1haWwiLCJXVCI6Mn0%3D%7C0%7C%7C%7C&sdata=4kjw1PyFmcZShstD6XPtsGQppUG6ohOp7CSozsnPH%2FE%3D&reserved=0) on the Privacy Act Reforms will have updates as more information becomes available.

1. **What do you see as the main privacy harms that could arise from generative AI?**

Privacy harms arise in different ways at different stages of the development and deployment of generative AI. Some main ones include:

* **Developers’ choice of training data** – most generative AI systems are trained on large volumes of data scraped from the open internet, often including personal information without notice or consent. Most companies selling AI systems will not provide detailed information about the training data they have used and whether it was collected lawfully or ethically.
* **Developers capturing queries for model training** – Most generative AI services aimed at enterprises don’t have this problem, but it is common for consumer-grade generative AI services to capture and use queries (including personal information) for model training. In most cases, agencies will not be authorised to provide personal information to suppliers for this purpose.
* **Users relying on inaccurate or low quality outputs** – generative AI produces plausible, but often inaccurate responses to prompts. Because outputs are plausible, errors can be non-obvious and difficult to detect. Using generative AI in the context of administrative decision-making creates a real risk of unfair, inaccurate or poor quality decisions.

For more information, OVIC’s Public Statements on the use of personal information with ChatGPT and Microsoft 365 Copilot provide in-depth explanations of the privacy risks arising from large language model or chat – type generative AI.