COLLABORATION TOOLS AND PRIVACY

The rise of flexible working arrangements means that collaboration tools, such as videoconferencing and instant messaging tools, as well as cloud-based document creation and sharing services, are becoming increasingly essential to facilitate day-to-day collaboration within businesses and government. However, the ability of collaboration tools to collect, store and transmit great amounts of personal information poses privacy risks.

The purpose of this guidance is to assist Victorian public sector (**VPS**) organisations consider their privacy obligations when implementing and using collaboration tools, focusing on instant messaging and videoconferencing tools. The guidance also references important information security and record-keeping considerations.

This guidance is designed to be general in nature and OVIC is unable to recommend or endorse a particular tool, or comment specifically on a tool’s privacy policy or security practices.

VIDEOCONFERENCING AND INSTANT MESSAGING IN THE PUBLIC SECTOR

Videoconferencing can be used to provide face-to-face contact for teams working remotely and to also facilitate remote learning. Popular programs or collaboration tools used by organisations may include Microsoft Teams, Cisco Webex Meetings, Google Meet, Apple FaceTime and even open source tools, like Jitsi. Many videoconferencing services also offer a chat or instant messaging function. Other popular instant messaging tools include Slack or WhatsApp.

When implementing and using videoconferencing and instant messaging tools, VPS organisations need to consider relevant information handling obligations, under the following legislation:

* *Privacy and Data Protection Act 2014* (**PDP Act**);
* *Freedom of Information Act 1982* (**FOI Act**);
* *Public Records Act 1973*; and
* *Surveillance Devices Act 1999* (**SD Act**).

CONSIDERATIONS BEFORE IMPLEMENTING COLLABORATION TOOLS

Determine the purpose and scope for the use of collaboration tools

Organisations should determine the purpose and scope according to their unique business needs *before* implementing videoconferencing or instant messaging tools. The requirements for privacy, information security and record-keeping will vary between organisations using videoconferencing or instant messaging tools for different communication purposes.

Conduct privacy impact and security risk assessments and review periodically

Before implementing any videoconferencing or instant messaging tools, organisations should conduct a privacy impact assessment (**PIA**), as well as a security risk assessment (**SRA**).

A PIA is a tool that can assist organisations understand and evaluate the impact on individuals’ information privacy posed by collaboration tools. Conducting a PIA will help organisations:

* identify whether their practices are consistent with the Information Privacy Principles (**IPPs**) under the PDP Act;
* identify any privacy risks that many arise;
* recommend steps to mitigate privacy risks; and
* outline the flow of personal information between relevant parties.

A PIA template and guide to assist organisations is available on [OVIC’s website](https://ovic.vic.gov.au/privacy/privacy-guidance-for-organisations/).

Conducting a SRA will assist organisations identify broader security risks arising from the use of collaboration tools. As well as obligations under the IPPs, many VPS organisations have obligations to ensure the security of public sector data under Part 4 of the PDP Act. More information about SRAs and information security obligations for VPS organisations is available on OVIC’s [website](https://ovic.vic.gov.au/data-protection/for-agencies/vpdsf-resources/).

Organisations may have their own guidance on managing privacy and security risks when using collaboration tools and OVIC’s PIA template, accompanying guide and information about SRAs should be read with any organisation-specific guidance. Organisations should also consult their privacy officer or privacy team when assessing the risks of using collaboration tools.

Any PIAs or SRAs conducted by agencies should be reviewed at least annually, to ensure the assessments reflect the way personal information is collected, used and transmitted through the collaboration tools. PIAs and SRAs should also be revisited if there is a change to the way organisations use the collaboration tools, or switch to new tools.

Develop internal terms of use policies

A terms of use policy (**TOU Policy**) should be made available to all staff prior to commencing office-wide use of collaboration tools. There is no single formula for a TOU policy, and each organisation will have to consider their specific context. Generally, the policy should:

* define the scope of use for the collaboration tool (for example, internally within an organisation, for meetings with external stakeholders, or for delivering training), clearly state which devices and programs it applies to, the purpose(s) of the collaboration tool and a description of the tool;
* contain a privacy policy and/or a collection notice detailing the collection, use, handling and disclosure of users’ personal information, in both the initial set up and ongoing use of the collaboration tool;
* outline user responsibilities according to intended purpose of the collaboration tool;
* outline what is considered to be appropriate and inappropriate use of the collaboration tool, with reference to other relevant workplace policies, such as workplace bullying, harassment and discrimination policies;
* inform users of the storage process and retention period of their personal information shared via the collaboration tool;
* inform users of the location where their personal data collected or shared via the collaboration tool will be stored;
* inform users how they can access their personal information stored by the collaboration tool;
* inform users of their security obligations when using the tools, including understanding the value of the information they share;
* explain that all business-related communication is subject to recordkeeping requirements regardless of the tool used and advise users of the desired way of creating records (for example, formal methods such as email should be used when recording business decisions);
* inform users that the information shared via the collaboration tool may be accessed under the FOI Act; and
* explain if (and what) disciplinary action may be taken if the TOU Policy is not adhered to.

Convey clear expectations for use to employees

As a complementary measure to the development and distribution of an internal TOU Policy, staff should have expectations for use made clear to them via initiatives like internal training sessions, including, if possible, access to ‘best practice’ guidance for using collaboration tools in a manner that respects privacy. Internal training sessions may explain the obligations of staff members under the TOU Policy in more depth and provide staff an opportunity to ask questions about their obligations when using collaboration tools.

COMMON PRIVACY AND SECURITY RISKS WHILE USING COLLABORATION TOOLS

Transborder data flows

Many collaboration tool providers store personal information collected in the cloud or in offshore data centres. VPS organisations should have an awareness of where staff members’ personal information is being stored, as well as the personal information of clients and service users (if relevant) and carefully consider the privacy risks associated. As well as considering transborder data flows while conducting a PIA on an organisation’s chosen collaboration tool, the location and storage of personal information should be considered during procurement and negotiated with vendors, if possible.

Organisations should be assured that they satisfy one of the grounds under IPP 9 for any transborder data flows.

Unclear privacy policies and terms of use

Some collaboration tools may have vague or insufficient privacy policies. Conversely, some tools may have overly complicated or legalistic privacy policies or terms of use. Where possible, VPS organisations should choose collaboration tools that demonstrate a commitment to privacy by having clear and accessible privacy policies, that are transparent about the way personal information is collected, used and shared with other parties.

Secondary uses or disclosures of personal information

It is important for organisations to consider the purposes for which personal information will be used or disclosed both by the organisation itself and the collaboration tool provider. These uses or disclosures should be outlined in the organisation’s TOU Policy.

Many collaboration tool providers will share personal information with subsidiaries or subcontractors to deliver the service or share personal information with third party advertisers. Organisations should therefore refer to the provider’s privacy policy, explore any uses or disclosure of personal information in their PIA on the chosen tool, and consider whether there are any settings that can be changed, or negotiations with vendors to adjust the amount of personal information shared before using the collaboration tool.

Inadvertent disclosure of official information

Organisations should ensure staff are aware of their information security obligations while discussing or sharing certain information via collaboration tools.

Many organisations have policies that collaboration tools should, where possible, only be used to facilitate day-to-day informal discussions and collaboration between staff and that business decisions should be communicated via email, to limit the potential for official information to be inadvertently disclosed via collaboration tools. This can also help to ensure that the organisation’s record-keeping obligations are being met.

Organisations should encourage staff to be aware of any official information that may be inadvertently captured via videoconferencing tools, such as in the background of a videoconference call.

Resources are available on OVIC’s [website](https://ovic.vic.gov.au/data-protection/framework-vpdsf/) to assist organisations understand their information security obligations.

Recording meetings held via collaboration tools

Most collaboration tools, such as Microsoft Teams, Cisco Webex Meetings, and Google Meet have the functionality to record meetings. Before choosing to record meetings, organisations must ensure there is a legitimate purpose for doing so. Recording meetings simply because the functionality is available may result in an over-collection of personal information.

In addition to the IPPs, organisations should also consider whether the initial recording and future uses of the recording comply with other obligations they may have, such as under the SD Act.

Users of collaboration tools need to be provided notice of the collection of their personal information via meeting recordings, in line with IPP 1.3. IPP 1.3 requires organisations to make users aware of the purpose for collection (in this case, recording meetings), where their personal information will be stored or disclosed, and the fact that they are able to gain access to their personal information (amongst other things).

It is good practice to allow users an alternative way to participate in the meeting if they do not want their personal information recorded. More information on notice of collection is available on [OVIC’s website](https://ovic.vic.gov.au/privacy/privacy-guidance-for-organisations/).To manage the risk of potential over-collection of personal information, organisations may also disable recording functions altogether.

RECORD-KEEPING AND FOI OBLIGATIONS

Record-keeping and retention of instant messaging logs

Although collaboration tools within organisations should only be used for informal, day-to-day discussions, to ensure record-keeping requirements are met, organisations may choose to retain logs of conversations via instant messaging for a certain time. Organisations’ record-keeping obligations are outlined in the relevant retention and disposal authorities, set by the Public Record Office of Victoria (PROV). Organisations are encouraged to refer to the [resources](https://prov.vic.gov.au/recordkeeping-government) available on PROV’s website.

Retaining logs of conversations can also allow organisations to conduct audits where necessary in response to workplace bullying, harassment or discrimination claims, for example.

Where necessary, employees may also be required to create records (such as a file note) to document important verbal arrangements made via collaboration tools, as well as business decisions and authorisations.

FOI obligations

Staff should also be provided clarity as to whether all or some conversations that occur via collaboration tools retained in organisations’ instant messaging log will form public records and be subject to FOI. Generally, all retained instant messaging logs will be a ‘document’ for the purposes of the FOI Act. Organisations can refer to OVIC’s [Practice Note](https://ovic.vic.gov.au/resource/practice-note-9-what-is-a-document-and-what-is-actual-or-constructive-possession/) on what a document is for the purposes of the FOI Act for further guidance.

IPP QUICK REFERENCE GUIDE

The below is a quick reference guide to assist organisations meet their obligations under the IPPs when using collaboration tools. This is not exhaustive, and organisations should conduct their own PIA to ensure they are meeting their privacy requirements.

The IPPs outlined are the most often engaged by the use of collaboration tools. Examples are included below, to illustrate privacy risks and mitigation strategies in practice.

Organisations are encouraged to refer to the [Guidelines to the IPPs](https://ovic.vic.gov.au/privacy/guidelines-to-the-information-privacy-principles/), available on OVIC’s website, for more information.

Collection

IPP 1.2 states that organisations can only collect personal information where it is lawful to do so. Organisations should consider other laws that may regulate the use of collaboration tools, such as the SD Act where organisations perform an audio-visual recording.

Users should be provided a notice of collection before, or as soon as practicable after, their personal information is collected and used to implement collaboration tools. IPP 1.3 outlines the matters that need to be covered when providing notice of collection. Guidance on collection notices is available on [OVIC’s website](https://ovic.vic.gov.au/privacy/privacy-guidance-for-organisations/).

As a rule, organisations should only collect the minimum amount of personal information necessary from users to implement collaboration tools.

The use of collaboration tools poses a risk of over-collection of personal information, for example organisations collecting more personal information than they planned to, collaboration tool providers requiring excessive personal information from users upon sign up, or meetings being recorded unnecessarily. Whether over-collection occurs as a result of users sharing unsolicited information or the organisation asking for more than the minimum amount of personal information required to operate the collaboration tool, all personal information collected by the organisation needs to be handled in accordance with the IPPs.

Use and Disclosure

* IPP 2.1 sets out the grounds for organisations to use and disclose users’ personal information to implement collaboration tools.
* Organisations should familiarise themselves with any secondary uses or disclosures of users’ personal information by the chosen collaboration tool and outline any secondary uses or disclosures in the collection notice provided to users.
* Where possible, organisations should negotiate relevant terms with vendors to minimise secondary uses and disclosures of personal information (for example, to third party advertisers).
* Videoconferencing can increase the possibility of personal information being inadvertently disclosed. For example, a staff member may be sharing their screen during a discussion and receive an email that is visible to others. Organisations should remind staff to be mindful of their surroundings and take precautions to limit the amount of personal information they share inadvertently when videoconferencing, such as disabling email notifications.

Data quality

* Organisations should alert users that the obligations under IPP 3 to keep personal information complete, accurate and up to date apply to communications via collaboration tools, particularly where a communication creates a formal public record.
* Organisations also need to ensure that any personal information they disclose about users to establish collaboration tools is complete, accurate and up to date.

Data security

* Organisations have obligations to protect the security of personal information under IPP 4. Some organisations may also have information security obligations under the Victorian Protective Data Security Framework and Standards, issued under Part 4 of the PDP Act.
* To meet these information security obligations when using collaboration tools, organisations may limit access to certain personal or account information only to those who require it (for example, an organisation’s IT Team) and provide staff clarity on the types of official information that are appropriate to disclose via collaboration tools.
* Collaboration tools may allow staff members to post personal information that others may access, such as a group chat or shared calendar. Depending on the type and sensitivity of the personal information, organisations should consider restricting access to those who need to know or informing users that others may access and view any personal information posted.

Unique Identifiers

* Depending on the collaboration tool, organisations may be required to assign a unique identifier to users, to access and create an account to use the tool.
* IPP 7.1 provides that an organisation must not assign unique identifiers to individuals unless the assignment of unique identifiers is necessary to enable the organisation to carry out any of its functions efficiently.
* Further, there are restrictions around organisations adopting the unique identifiers that may be assigned to users by the collaboration tools themselves, outlined under IPP 7.2.
* More information about unique identifiers is available in the [Guidelines to the IPPs](https://ovic.vic.gov.au/privacy/guidelines-to-the-information-privacy-principles/).

Transborder dataflows

* Many collaboration tools will share personal information with offshore third parties, such as subcontractors or subsidiaries, to assist in delivering the service. Providers of collaboration tools may also store personal information in offshore data centres or in the cloud.
* Organisations should be assured that they have grounds under IPP 9 to allow the transmission of users’ personal information outside of Victoria.
* Conducting a PIA will assist organisations understand whether their users’ personal information will be transferred outside of Victoria when using their chosen collaboration tool, and whether the organisation has legal authority to transfer this information. PIAs also require organisations to identify privacy risks, such as the storage of personal information offshore, and devise strategies to mitigate those privacy risks, such as binding collaboration tool providers to the IPPs under a State contract.