



# Privacy Foundations self-assessment tool

## About this tool

Having good privacy practices in your business or organisation brings many benefits, including building consumer trust and confidence that you are handling personal information safely and securely.

This Privacy Foundations tool has been designed for businesses who want to embed a culture of privacy, and who want to establish or improve privacy practices, procedures and systems.

The tool will help you to assess your business's current privacy practices by providing examples that may apply to your own circumstances. Following your self-assessment, the tool will make recommendations to implement in your day-to-day operations to achieve a more robust privacy culture. The results could also be used to create a Privacy Management Plan for your business.

The tool is intended to provide only a basic overview of privacy fundamentals and is not intended to offer a complete privacy assessment. It may assist businesses that do not have in-house privacy expertise to understand what they could focus on to improve their privacy maturity.

The tool does not assess compliance under the *Privacy Act 1988* (Cth) (Privacy Act). Public sector agencies and businesses that are covered by the Privacy Act may wish to use the OAIC's more in-depth Privacy Management Plan tool, as well as independent expert advice, to assess their privacy maturity against the Australian Privacy Principles (APPs).

Separate to any Privacy Act or State/Territory privacy obligations, the OAIC recommends that all organisations implement strong privacy management practices, as a core part of good business practice.

## What to expect

- **Assess your business against some foundational privacy questions** covering areas of core privacy good practice.
- **See practical examples** of what good privacy practice looks like.
- **Complete the assessment in 15-20 minutes** with guidance at every step.
- **Receive a privacy maturity score** and tailored recommendations for your business.

Use the OAIC's more in-depth Privacy Management Plan tool and/or independent professional advice, to assess your privacy maturity against the Australian Privacy Principles (APPs) — if required.

## How to use this tool

This tool contains two parts. Step 1 — Questionnaire and Step 2 — Action planning.

In Step 1, answer the questions, then use the answers you gave in Step 1 to help you calculate your privacy score in Step 2. You can also use your results in Step 2 to create a Privacy Management Plan.

**Note:** this is document is the simplified version of an automated excel-based tool. The information contained in this tool is the same as in the excel version but it does not provide any automations.

## Disclaimer



The tool provides a score of privacy maturity based on your self-assessment but is not a complete analysis of your business's privacy framework. Implementing appropriate privacy practices remains your responsibility. The OAIC does not guarantee that use of this tool will ensure compliance with any legal obligation, and businesses should regularly review and update their privacy practices, and seek professional advice where appropriate.

The information that you enter in this tool remains under your control and is not shared with the OAIC.

# Step 1 — Questionnaire

The following questions are designed to introduce foundational privacy concepts that are useful for your business to review. Each question is designed to assess your current state, and examples to guide your response.

Answer each question with **Yes**, **Partial**, or **No**, depending on how your business practices and procedures align with the examples given for that question.

- **Recommendations** (  ) appear where your business may wish to implement new privacy processes
- **Considerations** (  ) appear where you have some good practices but can improve further.

Mark the document with your answers as you go, using your preferred method (e.g. delete the incorrect response; use a highlight tool on the correct responses, or print and mark the correct responses).

## Accountability

**Objective:** There is a role or team in your business with accountability for privacy management

**Question:** Is there someone in the business who looks after privacy?

Answer	Score	Your recommendation
Yes: The legal team/in-house lawyer has that in their role; We have an external law firm or consultancy that advises on compliance requirements, with a key contact in the business who is accountable for decisions; We have a compliance team/person who looks after legal issues including privacy	1	Consideration ⓘ : Make a role or team responsible for ensuring there are repeatable processes in place which support good privacy practice.  Make a role or team responsible for ensuring that staff understand the business's privacy obligations (if applicable), and their role in complying with those obligations.
Partial: We have a team/person who manages our legal frameworks but I don't know how much they know about privacy	0.5	Recommendation ⓘ : A role or team should be given accountability for privacy matters in the business. That role or team should understand the business' privacy obligations (if applicable) and be appropriately resourced to be able to provide advice and guidance.
No: We don't have any legal, risk or compliance staff, and we don't receive external legal advice	0	

### Further information

You can find more information in [Chapter 1: APP 1 Open and transparent management of personal information](#)

# Transparency

**Objective:** The business communicates clearly with customers, clients or the public about how it handles personal information

**Question:** Do you have any external-facing documents that describe the personal information your business collects and how it uses and manages it?

Answer	Score	Your recommendation
Yes: We have a privacy policy and provide collection notices to individuals; We have a notice when we collect personal information explaining what we're doing with it and why	1	Consideration ⓘ : Make sure your privacy policy transparently describes your personal information handling processes.  Keep your privacy policy up to date. If your information handling processes change, make sure your privacy policy is still accurate and complete.  Make your privacy policy easy to read. Privacy policies should be written in plain English so that readers understand what you're telling them about their personal information.  Make your collection notices specific to that instance of collection and use of personal information. Make your notices easy to read.
Partial: We have something in our terms & conditions about what we're doing with personal information	0.5	Recommendation ⓘ↑ : Publish a privacy policy. Your privacy policy should describe in plain English what personal information you collect, how you collect that information, and how and why you use that information.
No: We don't have any external-facing documents about how we collect personal information	0	

## Further information

You can find more information in [Guide to developing an APP privacy policy](#)

# Training

**Objective:** Staff know how to appropriately handle and protect personal information

**Question:** Do you provide privacy training to your staff?

Answer	Score	Your recommendation
Yes: We have training modules on privacy and cyber security fundamentals	1	Consideration ⓘ : Have staff refresh their privacy and cyber training on a regular basis.  If there are team members who handle a high volume of personal information, or if the information they handle is sensitive, have those team members do further privacy training, or training tailored to their roles.
Partial: We have cyber training but not privacy; We mention information use in acceptable use training or policy; Privacy or personal information is mentioned in other unrelated training about how to use a system or process	0.5	Recommendation ⓘ : Train staff on privacy and cybersecurity fundamentals. Monitor and enforce training completion. Staff need to understand the business' privacy obligations (if applicable) and their role in handling personal information correctly.
No: We don't have any training in privacy; We only make staff sign an undertaking when they start with us that they will keep personal information secure	0	



## Further information

You can find more information in [OAIC Research and training resources](#)

## Managing privacy risk

**Objective:** The business assesses the privacy risks in new projects and processes.

**Question:** Do you have a process to consider privacy risk in projects?

Answer	Score	Your recommendation
Yes: We have a process for considering, assessing and mitigating privacy risks for new projects; Legal are responsible for signing off on any privacy risk in projects	1	<p>Consideration  : After implementation or go-live, review your projects and processes for privacy risks, especially if there have been changes in the scope or handling of personal information. Start with systems and processes that handle sensitive information or large volumes of personal information.</p> <p>Risk rate your processes and platforms, document it and keep it up to date, so that you have a clear understanding of your most significant privacy risks.</p> <p>Destroy information when you no longer need it. Obsolete personal information is an unnecessary risk to the business, and the individuals to whom the information relates.</p>
Partial: We discuss privacy for new projects but there isn't a process; We consider information/data security for new projects, but not all aspects of personal information risk	0.5	<p>Recommendation  : Create a checklist of personal information risks to consider early in a project when it becomes clear that personal information will be involved. Then, discuss ways to mitigate those risks.</p> <p>Have legal, or another role with responsibility for overseeing privacy compliance, sign-off on new projects or processes that involve personal information.</p>
No: We don't consider privacy risk in new projects or processes	0	

### Further information

You can find more information in [Guide to undertaking privacy impact assessments](#)

## Managing third-party risk

**Objective:** The business assesses the privacy risks of third-party solutions or services that may handle personal information.

**Question:** Do you have a process for assessing a third-party for privacy risk when procuring their solution or service?

Answer	Score	Your recommendation
Yes: We have a process for considering third-party privacy risks; third-party privacy risks inform whether we procure, or how we configure and implement a solution or service; We include terms in contracts with third parties about how personal information is handled and have mechanisms in place to ensure the third-party obligations are being fulfilled	1	<p>Consideration ⓘ : Review your services or solutions for new privacy risks, especially if there are changes in the scope or handling of personal information. Start with systems and process that handle sensitive information or large volumes of personal information.</p> <p>Risk-rate your third-party vendors. Document your risks and keep it up to date so that you have a clear understanding of your most significant privacy risks.</p> <p>Periodically follow-up with third-party vendors to monitor their privacy practices.</p>
Partial: We discuss third-party privacy risks but it's not comprehensive and there isn't a process; We review agreements with third parties for general compliance and commercial risks but always accept the third parties' privacy terms	0.5	<p>Recommendation ⓘ↑ : Create a list of third-party risks to discuss when considering procurement of a new system or service which involves the handling of personal information. Then, discuss ways to mitigate those risks.</p> <p>Have legal (or another role with responsibility for overseeing privacy compliance) undertake due diligence on how third parties handle personal information for signing off on new vendors. Include contractual clauses for how third parties must handle personal information, and implement processes to monitor and communicate about this.</p>
No: We don't consider third-party privacy risks	0	

## Further information

You can find more information in [Guide to securing personal information](#)

## Collection

**Objective:** The business only collects the personal information it needs for its operations, and no more.

**Question:** Do you only collect the minimum amount of personal information you need to carry out your business?

Answer	Score	Your recommendation
Yes: We make sure we have a clear business purpose for the personal information we collect before we collect it from individuals; We don't collect personal information if de-identified data will be sufficient	1	Consideration ⓘ : Proactively design your collection processes to collect the minimum amount of personal information. For example, if you don't have a clear business purpose to collect an individual's full birthdate, then don't collect this information. If your business purpose can be satisfied by collecting a birthday month, design your form so that it only accepts a month.
Partial: We do consider how to reduce the amount of personal information we collect but there is no process and it's not done consistently	0.5	Recommendation ⓘ : Before you collect information, consider whether de-identified information would be adequate for the purpose you are collecting it.
No: We don't think about how to reduce the personal information we need before we collect it	0	If you do collect personal information, make sure you have a clear business purpose for the information you request from individuals. Make data minimisation a part of your process for designing data collection channels.

### Further information

You can find more information in [Collection of personal information](#)

## Sensitive information and consent

**Objective:** The business gets consent for the collection, use and disclose of sensitive personal information.

**Question:** Does your business inform individuals why it is collecting sensitive information and seek consent for collection?

Answer	Score	Your recommendation
Yes: We seek consent before collecting sensitive information and keep track of consents we capture from individuals; We make sure that the consents we capture are meaningful and that we comply with them when we use and disclose personal information, including for direct marketing; Or we don't collect any sensitive information	1	Consideration ⓘ : Review your collection notices and make sure individuals are clearly informed what they are consenting to and why. Do not bundle multiple consent requests together, or force users to consent to a range of uses and disclosures. Try to ensure consent is informed, voluntary, current and specific.  Provide individuals with a way to withdraw their consent, and ensure you have processes to action their request within a reasonable timeframe.
Partial: We inform individuals what we're collecting and why, but we don't specifically call out sensitive information	0.5	Recommendation ⓘ : Sensitive information is an especially protected class of personal information and requires a higher level of protection and consents to collect and use. Therefore, you need to make sure you are collecting and honouring the consents.
No: We don't know what would make personal information sensitive; We don't collect consents; We collect consents but we don't do anything about them	0	Information about someone's health or biometrics, religious beliefs, sexual preferences or political views are some examples of sensitive information.  You should have a process by which you can capture the consent of individuals and can tie that consent to how you use and disclose that individual's information.

### Further information

You can find more information in [What is personal information](#)

## Managing use and disclosure

**Objective:** The business only uses and discloses information for the purposes it has told individuals it will.

**Question:** Does your business only use and disclose personal information for the purpose you collected it (and that you notified individuals about)?

Answer	Score	Your recommendation
Yes: We know what purposes and disclosures we've notified individuals about and we make sure we don't use the information for other purposes (unless an exception applies); We keep track of the uses and disclosures we've notified individuals of; We keep track of how we use and disclose personal information	1	Consideration ⓘ : Regularly review your privacy policy and collection notices, and update them if your uses and disclosures change.
Partial: We broadly know what we've notified individuals of and it's generally correct, but we don't have a process for managing/oversight of use and disclosure	0.5	Recommendation ⓘ : Your business is 'using' personal information if you control how the information is handled; Your business 'discloses' personal information if you give access to it, or show it to another individual, organisation or agency.
No: We don't understand the difference between use and disclosure; We don't have a clear idea of what we've notified individuals about; We don't have any external notices; We don't think about how we've notified individuals when we use or disclose personal information	0	Review your privacy policy and collection notices. Make sure they are complete and accurate in their description of your uses and disclosures.  Keep a register of your collection notices, privacy policies, and their dates and versions, so that you understand what you've notified individuals of.

## Further information

You can find more information in [Use and disclosure of personal information](#)

## Direct marketing compliance

Objective: That the business has opt-outs in its direct marketing and honours them.

Question: Do you have opt-outs in your direct marketing?

Answer	Score	Your recommendation
Yes: We have opt-outs in our direct marketing and a process to ensure action of those opt-outs; Or we don't conduct direct marketing	1	Consideration ⓘ : Let individuals withdraw their consent, and have a process to action their opt-out in a timely fashion.
Partial: We include opt-outs in our direct marketing and process them manually and/or occasionally	0.5	Recommendation ⓘ↑ : Create a process to ensure that opt-outs are recorded and actioned in a timely fashion.
No: We don't include opt-outs in our direct marketing; We have opt-outs in our direct marketing but they have no impact on who we market to	0	

### Further information

You can find more information in [Direct marketing](#)

## Information inventory

**Objective:** The business has a documented inventory/list of its personal information holdings, including where the information is stored, what it is used for and how long it should be kept.

**Question:** Do you have an inventory of your personal information holdings?

Answer	Score	Your recommendation
Yes: We have an up-to-date inventory of our personal information holdings	1	Consideration ⓘ : Keep your information inventory up to date.  Add information to your inventory if it helps you to understand and manage your privacy risks. Other information you could add to your inventory include risk ratings, sensitivity labels, and whether third parties are involved.
Partial: We know what personal information we have, but it's not documented; We have documented what personal information we hold, but it's not up-to-date; We have documented what personal information we hold, but the information about where it's stored and/or what it's used for is incomplete or outdated; Information about the personal information we hold is spread across multiple documents and systems	0.5	Recommendation ⓘ↑ : Document the personal information the business collects, uses and discloses. Document where that personal information is stored.  Document retention periods for the personal information you hold so that you can destroy personal information when the business no longer needs it.
No: We don't have a good idea of what personal information we hold	0	

### Further information

You can find more information in [What is personal information](#)



## Cyber security

**Objective:** The business has a process to effectively manage cyber risk.

**Question:** Do you have processes for managing cyber risk?

Answer	Score	Your recommendation
Yes: We have a cyber security team; We have an IT team with oversight of cyber security; We have cyber security processes including training and use of basic access controls like passwords and multi-factor authentication; We oversee contractors who provide our cyber security, who report regularly to us and their cyber security responsibilities and services are clearly set out in a contract	1	<p>Consideration ⓘ : Implement data loss protection controls. Controls can stop unauthorised export or sharing of information from business systems and can prevent personal information inappropriately leaving the control of your business. These can include restrictions on large attachments to emails, or restrictions on emails to non-business emails. Focus on systems holding high volumes of personal information, or systems holding sensitive personal information.</p> <p>Personal information is often stored in back-ups and obsolete systems. Ensure these systems are secured and well managed. If possible, destroy the personal information in these backups or systems.</p>
Partial: IT would deal with any cyber problems but there's no process; We have cyber risk management tools like multi-factor authentication but no policies or procedures; We have a contractor that provides our cyber security but we don't have clear policies and procedures for overseeing their work and the contract is not clear regarding the extent of their services and their responsibilities	0.5	<p>Recommendation ⓘ : Give a role accountability for overseeing cyber risk in the business.</p> <p>Implement cyber security controls on systems that store personal information. Controls could include role-based access controls and multi-factor authentication.</p> <p>Document cyber procedures to ensure there are consistent processes in place to manage incidents, access, data and system security.</p>
No: We don't have any cyber processes or a role with oversight of cyber security	0	

## Further information

You can find more information in [Guide to securing personal information](#)

## Data breach management

**Objective:** Staff know how to identify and escalate a data breach.

**Question:** Do you have processes to identify and manage a data breach?

Answer	Score	Your recommendation
Yes: We have a data breach response plan; We have a standard process to escalate any privacy/information security concerns	1	Consideration ⓘ : Train legal/senior staff in how to manage a data breach so that they can respond quickly and decisively.  Document a data breach response plan that assigns roles and responsibilities for identifying, containing, assessing, notifying (the OAIC and affected individuals) and reviewing a data breach. Regularly test the plan.
Partial: Staff know to let legal/senior staff know if they have any concerns about information security, but there's no documented policy or process	0.5	Recommendation ⓘ : A data breach occurs when personal information is accessed or disclosed without authorisation or lost.  Train staff in recognising and escalating notice of a data breach.
No: We don't know what 'data breach' means; We don't have any processes for a data breach; We've never thought about how to manage a data breach; Staff wouldn't know what a data breach is	0	Assign roles and responsibilities to legal/leadership in responding to a data breach. Include staff, like IT, whose support is necessary not only to prevent a breach, but to identify affected individuals. Document the process.

### Further information

You can find more information in [Data breach preparation and management](#)

## Secure and timely destruction or de-identification

**Objective:** The business securely destroys information when it no longer needs it.

**Question:** Does your business regularly destroy personal information it no longer needs?

Answer	Score	Your recommendation
Yes: We have a register or schedule which tracks when we can destroy personal information; We regularly destroy (or de-identify) personal information we no longer need	1	Consideration ⓘ : Consider backup tapes and archived information. These may also hold personal information which are eligible for destruction.  Document when and what information is destroyed so that you know destruction is happening regularly, and that it is happening in accordance with your approved process.
Partial: We have a schedule which records when we can destroy personal information but we don't regularly do it; We periodically destroy information but there is no process or it is not done regularly	0.5	Recommendation ⓘ : Consider how long you need various types of personal information to carry out your business, then create a disposal schedule to document when information should be destroyed. Create a process to regularly flag these items for destruction, and destroy them.
No: We don't know when we should destroy personal information; We don't destroy information	0	Give a role or team responsibility for regularly destroying personal information your business no longer needs.



### Further information

You can find more information in [Guide to securing personal information](#)

## Enquiries, complaints and requests

**Objective:** The business can respond to a complaint or a request from an individual that relates to their personal information.

**Question:** Could you give an individual the information they need if they ask about how you handle their personal information?

Answer	Score	Your recommendation
Yes: Staff can recognise a privacy complaint or an access/correction request and know how to manage it; Staff can recognise a privacy complaint or request and know who to direct it to	1	Consideration  : Processes for responding to complaints and access/correction requests are clearly understood.  You should respond within a reasonable time (the OAIC recommends 30 days). Document and implement processes to ensure your business can respond in a reasonable timeframe.
Partial: Staff know who to refer requests to but they may not consistently recognise a privacy complaint or request	0.5	Recommendation  : Implement a process to enable individuals to make a privacy complaint, to request access to the personal information you hold about them, or to correct that information.
No: There is no process. Staff members handle the requests themselves	0	Make sure staff are trained in the process, document the process and respond in a timely manner.

### Further information

You can find more information in [Handling privacy complaints](#)

## Step 2 — Action planning

### About this step

This step enables you to create an optional Privacy Management Plan based on your questionnaire responses. The plan includes your privacy score, outcomes, and space to document an action plan.

This completed document could serve as your business's Privacy Management Plan and can be saved and printed for your records.

### Privacy score

Add up the scores you received against each question to calculate your privacy score.

Score	Maturity level	Descriptor	Advice
0-3	Initial	You are just beginning to consider privacy processes in your business.	Focus on implementing the recommendations in this tool and other resources to establish foundational privacy practices.  You may also benefit from additional professional advice, and/or from using the OAIC's more in-depth Privacy Management Plan tool.
4-6	Commencing	You have some privacy processes in place, but they are not systematically embedded across all areas of your business.	Prioritise the recommendations to build a consistent approach to privacy management.  You may also benefit from additional professional advice, and/or from using OAIC's more in-depth Privacy Management Plan tool.
7-9	Developing	You have established some strong privacy processes while others need development.	Work through the remaining recommendations and begin considering the improvements suggested.

			You may also benefit from additional professional advice, and/or from using OAIC's more in-depth Privacy Management Plan tool.
<b>10-12</b>	Refining	You are meeting most or all of the foundational privacy processes for businesses outlined in this tool	Focus on continuing to enhance your privacy maturity and prepare for more advanced requirements.

<b>Your score:</b>	
--------------------	--

## Action plan

Record the advice you received in response to each question, then use the **Action**, **Assigned to**, and **Due date** columns to create your implementation plan.

For more information on the APPs, refer to [Australian Privacy Principles guidelines](#).

Question	Recommendation	Action	Assigned to	Due date
Accountability				
Transparency				

Question	Recommendation	Action	Assigned to	Due date
Training				
Managing privacy risk				
Managing third-party risk				

Question	Recommendation	Action	Assigned to	Due date
Collection				
Sensitive information and consent				
Managing use and disclosure				
Direct marketing compliance				

Question	Recommendation	Action	Assigned to	Due date
Information inventory				
Cyber security				
Data breach management				
Secure and timely destruction or de-identification				

Question	Recommendation	Action	Assigned to	Due date
Enquiries, complaints and requests				