



Your professionalism and commitment to managing information with integrity helps to build public trust in the way the Australian Government delivers programs and services. Start with the six key information-related actions outlined below. These apply to the APS, contractors, consultants, reservists and volunteers.

1. Know your responsibilities

- Whatever your role, every thing you create, save, use or share will be an [official Australian Government record](#).
- Act with [integrity](#). You must keep a record of decisions made, the reasons and anything relied upon when preparing advice.
- Find out what your [information management-related obligations](#) are in your agency and how these relate to the [Building trust in the public record policy](#).
- Some information is valuable and needs to be kept forever. Become familiar with the [legal authorities](#) and [standards](#) that apply.
- Senior executives, managers and supervisors have responsibility for reinforcing good practices to their staff and leading by example.

What's in it for me? I am accountable and my agency can withstand any scrutiny.

2. Control the risks

- Secure the privacy of others. Agencies [must handle information](#) as per the *Privacy Act 1988*.
- Keep accurate records. Users can inadvertently make mistakes when they rely on misleading, incomplete or inaccurate data, information and records to make decisions.
- Poor information practices have consequences. They can adversely affect the rights and entitlements of the general public to access government support.
- Guard against information threats. Information security is [governed by 4 core policies](#) under the Protective Security Policy Framework and is relevant under the [Information Security Manual](#).
- Prevent unlawful access to or release of information. Agency information can be subject to scrutiny, review, appeal or legal proceedings. Understand when the [Office of Australian Information Commissioner](#) and the [National Archives of Australia](#) enable access.
- Information has value. Make it difficult [for fraudsters](#) to compromise or steal information. [Agencies are obliged](#) to manage their fraud risks.

What's in it for me? These tips help to mitigate risks to me as well as my agency.

3. Listen to the experts

- Your agency's information management experts can provide advice on the best practices used to manage information.
- Experts can help identify and mitigate information management risks.
- Successful program, policy or project delivery relies on well-considered plans and use of information. Experts may be able to guide you.
- Consult agency experts to improve [business systems](#) and processes, [enhance interoperability](#) or break-down organisational information silos.

What's in it for me? I can get help when I need it.

4. Make information searchable and reusable

- Use agency standards and business rules to describe information consistently to make it easier to search; avoid contributing to 'needle in a haystack' scenarios.
- Learn where information must be officially saved so it can be accessed and re-used by others in your agency.
- Proper management of information can lead to greater productivity.
- All government information should be protected and controlled. Be confident that you are doing the right thing.

What's in it for me? Information I create and save can be discovered by those who need it.

5. Develop skills

- There are [APSC resources](#) that can help you understand what integrity means and what is expected of you.
- Self-assess your [information and data capabilities](#) and identify new learning pathways.
- Participate in training opportunities provided by your agency's information and data managers.
- Find out more about our videos and eLearning modules by visiting our [training resources web page](#).
- Support your team by contributing to its [information governance skills](#) and [information management capabilities](#).

What's in it for me? I have the skills-set and confidence to manage information with integrity.

6. Think ahead

- [Legal instruments](#) are used by agencies to determine what information needs to be retained, why and for how long.
- Keeping records beyond their retention increases the risk of data spills and can lead to reputational damage.
- Consider the [storage](#) and [preservation needs](#) of your information. Formats can quickly become obsolete. Get help to migrate information to a new format to ensure it is accessible.
- Seek advice to prevent information assets from being lost, stolen, damaged or unlawfully accessed.
- Others may need to access, use or re-use the information you control. Revisit actions 1 to 5 to ensure you manage information with integrity.

What's in it for me? The information I create is available for as long as it is required under my agency's business rules.