# Privacy obligations

**On this page**



As a senior executive, you play a positive role in managing private personal and health information as an agency asset. By doing so, you will encourage others to comply with NSW privacy legislation and contribute to your agency’s success and reputation.

You need to familiarise yourself with your responsibilities in relation to privacy management under the ***Privacy and Personal Information Act 1998*** and ***Health Records and Information Privacy Act 2002***.

## Implementing a ‘privacy by design’ approach

Your agency should have a privacy governance framework in place. The framework helps clarify each person’s role in managing privacy and ensures that everyone is held to account. Appropriate and adequate policies, processes, systems and reporting tools help foster a culture where staff members view privacy as an asset, not as a liability.

Use the following checklist to ensure that your workplace is managing privacy for the benefit of your agency and the people of NSW.

- Do roles in my agency have clearly articulated privacy management responsibilities? Are the people in these roles aware of their own individual accountabilities? Remember that privacy is everybody’s business.
- Do I have a forum where I can discuss privacy management issues and risks pertaining to my agency? You are ultimately responsible for ensuring that your agency is adequately managing privacy.
- Does my agency have any mechanisms in place to detect privacy breaches? This may include an internal incident management framework that encourages staff members to report privacy breaches when they occur, allowing appropriate steps to be taken to remediate the breach.

- Does my agency have any mechanisms in place to prevent a privacy breach from occurring? This may include IT security safeguards to prevent the inadvertent disclosure of information.
- Are my agency's privacy management plans, policy and procedures adequate and up to date?
- Is privacy considered a part of my agency's change management framework?

# Privacy responsibilities

The mix of roles and responsibilities will vary depending on your agency's size and circumstances.

When privacy is being adequately and effectively managed:

- Audit and Risk Committee and security experts identify and monitor privacy breaches, and agency learnings, and ensure risk frameworks adequately consider the impacts of privacy risks
- your agency's Privacy Contact Officer develops, updates and administers privacy management plans, procedures, and internal reviews, and is sufficiently knowledgeable to inform agency staff and members of the public of privacy issues
- managers consider privacy issues, implement privacy policies and procedures, and manage the handling of personal information across their business unit activities (projects, programs, systems and services)
- project managers consider a privacy by design approach to all new projects and implement privacy risk mitigations and considerations from the start of projects
- front line staff members comply with the policies and procedures set out by the agency
- your Human Resources function inducts new staff members and trains them about the agency's privacy policies and procedures
- your Governance and Legal functions ensure and manage legal compliance, assist with reporting, and provide advice about the agency's privacy obligations and needs for flexibility.

The Information and Privacy Commission has **privacy resources for agencies** and **eLearning modules for individuals** available to assist you to comply with your duties under the law.

Some other tools to get started:

**Essential guidance toolkit on information access and privacy fundamentals**
Key guidance for agencies to help them meet their requirements under the GIPA Act, including specific information for senior executives. →

**Digital projects**
Guidance on the information access and privacy issues agencies should consider when designing and implementing a digital project. →

**Privacy by design**

Information on privacy by design, which ensures that good privacy practices are built into your agency's decision-making processes, and the design and structure of your information systems, business processes, products and services. →

**Data Breach Prevention Checklist**

A useful list of internal checks where you can measure your current level of preparation for data breaches. →

**Information governance self-assessment tools**

These tools help agencies assess their systems and policies to make sure they are complying with their privacy and information access requirements. →

**Privacy e-learning modules**

Complete these modules to learn more about privacy protection and the right to information. →

# Data breaches

In the case of a data breach at your agency, it is important to take action quickly.

Proactively reporting breaches sends a strong message to the public that your agency is committed to promoting a culture of privacy protection and has the necessary systems and processes in place to ensure accountability if a breach occurs.

Proactively and voluntarily addressing breaches where they do occur plays a critical role in maintaining public trust in an agency's ability to manage people's personal information.

Currently, NSW operates under a voluntary data breach notification scheme. Public sector agencies can report breaches to the NSW Privacy Commissioner. You should also be working with your privacy and governance teams to ensure steps are being taken to mitigate any further risks of harm to individuals affected by a breach.

There are currently plans to introduce a Mandatory Notification of Data Breaches Scheme in NSW.

You can learn more about the current voluntary scheme and any updates on the mandatory scheme by visiting the **Information and Privacy Commission website**.

# Legislative frameworks

NSW public sector agencies often need to collect, store and use personal and health information to provide services such as transport, health and education. Public sector agencies are legally required to abide by certain principles to ensure privacy is protected.

You must ensure you understand these core requirements.

The ***Privacy and Personal Information Protection Act 1998*** outlines how NSW public sector agencies must manage personal information and the functions of the NSW Privacy Commissioner. This Act applies to all NSW public sector agencies, statutory authorities, universities, local councils and other bodies whose accounts are subject to the Auditor-General's inspection and audit.

The ***Health Records and Information Privacy Act 2002*** outlines how NSW public sector agencies and health service providers manage the health information of members of the NSW public. This Act applies to agencies that are health service providers or that collect, hold or use health information.

This legislative framework is complemented by other mechanisms, including codes of practice, privacy management plans and complaints management protocols.