Privacy on Purpose

5-STEP PLAN

For Enhancing Information Management
and Privacy Act Compliance

INFORMATION
LEADERSHIP

Why Privacy Matters

In an increasingly digital world, New Zealanders rightfully expect their personal information to be treated with care, respect, and transparency. From schools and councils to private businesses and not-for-profits, every organisation that handles personal data has a legal – and moral – obligation to uphold the principles of the Privacy Act 2020.

Beyond compliance, safeguarding privacy builds trust. Whether you're responding to access requests, managing sensitive employee data, or using digital tools like Microsoft 365, OneDrive and Teams, how you handle information speaks volumes about your values.

But privacy doesn't manage itself. It takes deliberate action, embedded processes, and an organisation-wide culture of responsibility.

This 5-Step Plan for Enhancing Information Management and Privacy Act Compliance is designed to help your organisation go beyond box-ticking. It blends practical guidance with trusted local resources – like the Office of the Privacy Commissioner's e-learning tools and response calculators – to help you build systems that support both compliance and care.

Let's get started.

About us

Information Leadership is a Microsoft Modern Work and AI Cloud Partner, and 100% kiwi owned. With more than 20 years of experience, we provide digital workplace solutions that empower, transform and protect organisations in an AI-enabled world.

5-Step Plan

01 **Establish Awareness and Responsiblity**
Educate staff on privacy responsiblities and define roles

02 **Develop Integrated Policies**
Create policies addressing privacy principles and management best practices

03 **Implement Information Systems**
Optimise digital tools for better information management

04 **Embed Compliant Processes**
Set up accessible processes for handling complaints and breaches

05 **Continually Monitor and Improve**
Regularly review practices and stay updated on legislation

INFORMATION LEADERSHIP

5-Step Plan

01

Establish Awareness and Responsiblity

Educate all staff on their privacy responsibilities using resources like the Privacy Commissioner's free e-learning tools. These cover topics from Privacy 101 to reporting privacy breaches.

Clearly define roles and responsibilities for information management and privacy compliance, including the role of Privacy Officers.

Consider conducting initial Privacy Impact Assessments (PIAs) to identify potential privacy risks associated with current information handling practices.

02

Develop and Implement Integrated Policies and Procedures

Create comprehensive internal policies and procedures that address both the 13 Privacy Principles and broader information management best practices (drawing on areas like digital workplace strategy, record keeping, and content management).

Establish clear processes for handling access and correction requests, keeping in mind the Response Date Calculator from the Office of the Privacy Commissioner.

Develop a robust data breach response plan, outlining the steps for identification, containment, assessment, notification and review.

03

Implement and Optimise Information Management Systems and Practices

Review and optimise your organisation's use of digital workplace tools (e.g., Microsoft 365, SharePoint, Teams) to improve information organisation, accessibility, and security. Consider solutions that help solve content problems and reduce information silos.

Establish clear guidelines for document management, record keeping, and information retention, aligning with both legal requirements (including the Privacy Act and the Public Records Act, if applicable) and organisational needs.

04

Embed Complaint Handling and Breach Management Processes

Establish a clear and accessible process for individuals to lodge privacy complaints directly with your organisation first. Follow the guidance in "Handling privacy complaints: a step-by-step guide".

Ensure your data breach response plan is well-understood and regularly tested. Have clear protocols for determining if a breach is notifiable to the Privacy Commissioner and affected individuals.

05

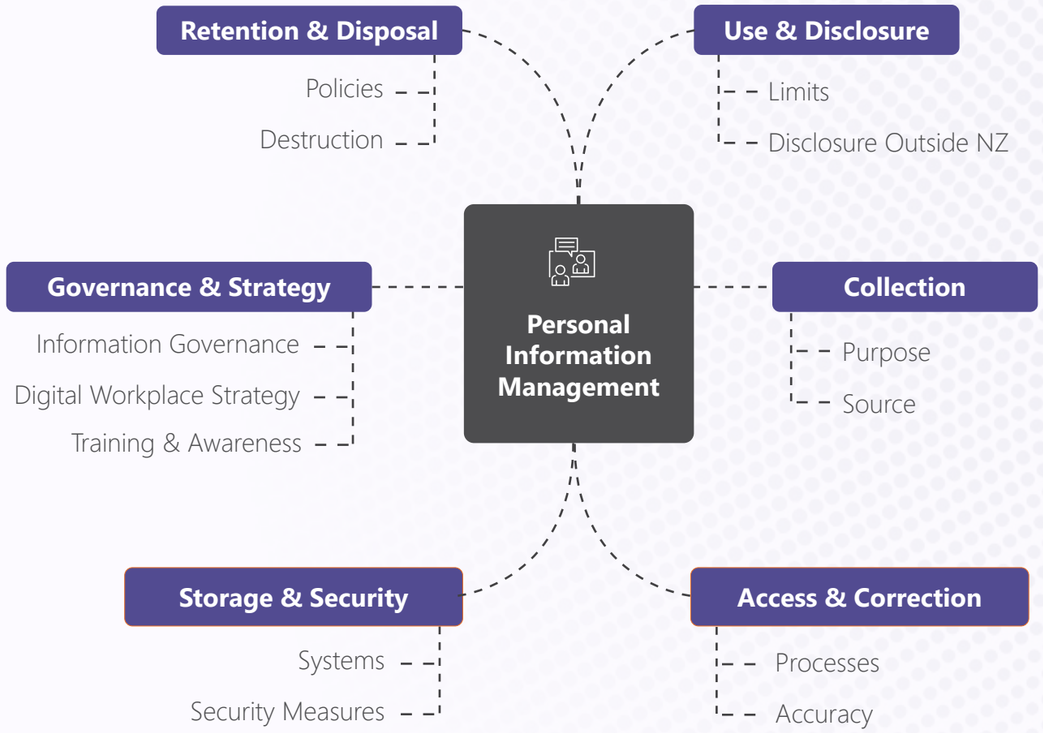
Continuously Monitor, Review, and Improve

Regularly monitor your information management practices and privacy compliance against your established policies and procedures, as well as the requirements of the Privacy Act.

Stay informed about updates to privacy legislation and guidance from the Privacy Commissioner.

Conduct periodic reviews of your policies, procedures, and systems to identify areas for improvement and ensure ongoing effectiveness. Consider conducting regular Privacy Impact Assessments (PIAs) for new projects and processes involving personal information.

Personal Information Managment and Privacy Compliance Framework



Services & Solutions

Information Leadership provides a comprehensive range of services and solutions designed to help organisations protect their information and meet compliance requirements. With over 20 years of expertise, we empower customers to elevate their privacy practices with confidence and control.

WORKSHOP & RESPONSE PLAN

Privacy on Purpose Workshop
A half-day workshop tuned for your organisation and aligned to the Privacy Commission guidelines.

Response Plan
A paint by numbers approach that guides your organisation through each of the 5 steps to create your plan for enhancing information management and Privacy Act compliance.

iWORKPLACE SOLUTIONS

Information Protection and Compliance
A suite of iWorkplace solutions that protect information and provide insights into how users interact with information, helping organisations understand and mitigate risks.

Content Retention and Disposal
Smart Records and Smart Labels automate the classification of content based on sensitivity and regulatory requirements, define retention periods, and securely delete content when it's no longer needed.

OneDrive Manager
Monitoring and improvement tools for mitigating OneDrive risk.

Permissions and Access Controls
Targeted permissions and access controls ensure that sensitive content is only accessible to those who need it, reducing the risk of unauthorised access.

Sensitivity Labels
Protect confidential and private information, ensuring that even if data is accessed by unauthorised individuals, it remains protected and unreadable.

Zero-Trust Security
Treats every access request as potentially hostile, enforcing multi-factor authentication (MFA), comprehensive endpoint management, and secure development practices.

iWorkplace Elements
Self-deployable options for high-risk information like contracts, personnel files, and policies and procedures.

Partner with us to protect your organisation's information with confidence — strengthen privacy, ensure compliance, and reduce risk with trusted expertise.

Get in touch today!
info@informationleadership.com
0800 001 800

INFORMATION LEADERSHIP

TOP TIPS

Privacy on Purpose

Don't need it, dispose of it!

Regularly review and dispose of unnecessary content to keep your workspace organised and boost security and compliance.

Implement access controls

Implement strong access controls to protect sensitive information and ensure only authorised personnel can access, modify, or delete data.

Classify with purpose

Use sensitivity labels to classify and protect your content, ensuring sensitive information is handled securely.

Education reduces risks

Educate employees on content retention and disposal to reduce risks of breaches and non-compliance.

Data privacy policies

Document your data privacy policies to ensure legal compliance and maintain stakeholder trust.

INFORMATION LEADERSHIP

GET IN TOUCH

0800 001 800
info@informationleadership.com
informationleadership.com
Follow us on LinkedIn

let's make work better