10 TOP TIPS to help Senior Managers and the Executive Team support a privacy culture

People are an agency's most important resource; their information is your most important asset. And public trust and New Zealanders' well-being should be your most important objective.

People will trust your agency and interact more readily if they have faith that you will handle their personal information with care because they can see you take privacy seriously and you respect them and the personal information they provide.

By law, every agency must have a Privacy Officer responsible for ensuring the agency complies with the provisions of the Privacy Act.

But good privacy practice is everyone's responsibility and must be understood and embraced agency-wide. All staff need to act responsibly, and in good faith. Managers can't hold their staff to account if their own knowledge and behaviours aren't up to scratch.

1. Set the tone from the top

- Foster a strong privacy culture by good governance and through leaders who are seen to lead by example.
- Build and maintain the trust of the community and of staff though accountability and transparency.
- Make good privacy practice a core agency value and "just the way we do things around here".
- Include privacy in your agency's Vision Statement and Code of Conduct to reinforce expectations.
- Set clear privacy expectations and requirements for employees in job descriptions and in the terms and conditions of all contracts with third parties.

2. Show you care

- Publish your agency's privacy impact assessments to show you value privacy and use appropriate safeguards.
- Consider publishing internal privacy policies and procedural documents on the public-facing agency website also for increased transparency.
- Publish clear instructions on how people can access their personal information, and tell them how they can contact you with any concerns or questions.

3. Support your team

- Consider your Privacy Officer one of your agency's most important strategic assets.
- Give them the tools and resources they need to get the job done and a clear mandate to educate, monitor,and respond.
- Support a robust Privacy Management Programme with defined accountability and assurance across the whole agency.

4. Walk the talk

- Make privacy training part of everyone's core duties – including for all your senior leaders and managers. Well-trained people will be your agency's greatest strength – poorly educated, unsupported staff your greatest weakness.
- Have a Privacy Champion on your ELT to support the Privacy Officer and help keep privacy alive on the Executive's risk radar.
- Visit your Privacy Officer (and their team) regularly and invite them to talk with the Executive Team also to make privacy more than just a metric.

5. Keep on the same page

- Ensure staff across the whole agency work together, rather than in silos to broaden understandings and build a consistent privacy culture.
- Build privacy into Key Performance Indicators for all staff across the agency, in all disciplines and in all roles.

6. Understand your vulnerabilities

- Identify privacy threats by carrying out regular risk audits, vulnerability assessments and penetration tests.
- Ensure any rules applied to staff are also being followed by any third parties acting on your behalf.
- Monitor for any new risks by including a dash-board assessment in regular internal reporting – things change!

7. Reduce the risk

- Assign clear roles for personal information handling, with audit, assurance and oversight responsibilities.
- Assign employee access and use controls on a need-to-know basis, matched to employee roles and functions.
- Where access can't practically be limited, monitor access to help identify inappropriate behaviour such employee browsing.

8. Spread the word

- Write privacy notices in plain language and publish them so they are readily accessible to staff and to the public.
- Provide regular messages to staff in weekly 'all staff' bulletins and updates to keep privacy front-of-mind.
- Take time to stop, look and listen by requiring regular reporting of privacy matters across the agency.

9. Be realistic, and reasonable

- Have a no-blame policy for privacy breach and incident reporting - Remember that no matter how good your policies and practices are, problems will always arise and you can't fix problems you don't know about. A no surprises approach is the best way to ensure no nasty surprises!
- When problems are identified, ensure resources are available to remedy the issue, and to provide ongoing assurance that mitigations work to prevent recurrences.

10. Trust but verify

- Make employees aware of the significant damage to your agency's reputation of any breach of confidence.
- Have policies that clearly state the consequences of negligent or malicious misuse of personal information so staff understand the potential repercussions.
- Trust your staff to do the right thing, and give them the tools to do so.