

Statement of Intent 2008/09

Office of the Privacy Commissioner

Te Mana Matapono Matatapu

Presented to the House of Representatives
Pursuant to section 139 of the Crown Entities Act 2004



Privacy Commissioner
Te Mana Matapono Matatapu

STATEMENT OF INTENT 2008/09
OFFICE OF THE PRIVACY COMMISSIONER
TE MANA MATAPONO MATATAPU

Presented to the House of Representatives
Pursuant to section 139 of the Crown Entities Act 2004

CONTENTS

Introduction.....	3
Nature and Scope of Functions.....	4
Privacy Commissioner Functions.....	4
The Operating Environment.....	6
Strategic Direction.....	7
Our challenge.....	7
Drivers.....	7
Government Priorities and Justice Sector Outcomes.....	7
Operating Intentions.....	9
i. Improved privacy awareness in the community.....	9
ii. Improved privacy standards and practice in government and business.....	10
iii. Individuals are equipped to resolve their privacy concerns.....	11
iv. New Zealanders' privacy is promoted through engagement at an international level.....	12
Managing in a Changeable Operating Environment.....	13
Risks.....	13
Environmental Scanning.....	14
Assessing Organisational Health and Capability.....	15
Service Performance.....	16
Outputs.....	16
1. Policy.....	16
2. Communications.....	17
3. Compliance.....	18

Financial Forecast Statements	20
Statements of forecast financial performance, position and cash flows for the year ending 30 June 2009	20
Statement of Forecast Service Performance.....	23
Statement of accounting policies.....	24

INTRODUCTION

The exponential growth of the digital environment, both in New Zealand and internationally, together with developments in science and telecommunications, present major challenges for the Office of the Privacy Commissioner. Phrases such as “surveillance society”, “identity management”, “social networking”, and “data-mining” have become common in media reports on the information revolution. People are becoming more aware and concerned about the “digital shadow” we all accumulate in day to day life and transactions.

The Office will focus on meeting these challenges and concerns in two main ways. We will work to raise public awareness of the need to protect personal information and provide tools for self resolution, advice and personal information protection. We will also work with government, business, and civil society domestically and internationally to improve their awareness that citizen and client trust depend on good personal information handling. Many tools are available to improve personal information handling, including cross-border co-operation, privacy enhancing technologies, codes of practice, regulation by government, or industry self-regulation. Good privacy practice is a business enabler and responsible stewardship will enhance the reputation of agencies holding big stores of personal information.

Our aim is to work constructively with government and business to build practical privacy protections, and to promote a culture of respect for individual privacy.

A handwritten signature in black ink, appearing to read 'Marie Shroff'. The signature is fluid and cursive, with a large, stylized 'M' and 'S'.

Marie Shroff
Privacy Commissioner

NATURE AND SCOPE OF FUNCTIONS

Protecting personal information and privacy is a complex area whose scope extends across government, business, the economy and society at large. Privacy is a human right that can, when managed in a careful way, be reconciled with potentially competing interests, such as efficiency in business. Finding that balance has become increasingly important, because a changing technological environment has opened new means and opportunities for government and business to acquire, manage and distribute personal information.

The Privacy Act 1993 takes a modern approach to the regulation of personal information through the application of principles. Openness, fairness and clarity of purpose are its themes.

Section 13 sets out many of the functions of the Privacy Commissioner. Other functions, including complaints and information matching, are set out elsewhere in the Privacy Act and in the provisions of other legislation.

Competing interests

The Privacy Act requires the Commissioner to have regard both to the privacy principles and the protection of important human rights and social interests that compete with privacy. These include the desirability of a free flow of information, and the right of government and business to achieve their objectives in an efficient way. The Commissioner must also take account of New Zealand's international obligations and consider any general international guidelines that are relevant to better protection of individual privacy.

Independence

The Privacy Commissioner is independent of the Executive Government in carrying out her functions and in investigating complaints, including those against ministers or their departments. Independence is also important when carrying out inquiries into privacy issues, examining the privacy implications of proposed new laws and information-matching programmes and in dealing with the private sector.

The Office has a total expenditure budget of \$3,480,000 with an operating grant of \$3,148,000 (excl GST); a staff of 31.8 FTEs; and two offices, in Wellington and Auckland. Additional funds are provided through funding by external agencies and the provision of services.

Privacy Commissioner Functions

The Privacy Commissioner has wide ranging functions.

Legislation and policy

One of the Commissioner's key roles is to comment on legislative, policy or administrative proposals that have some impact on the privacy of individuals. The Office assists public and private sector agencies to reach reasonable goals in a privacy respectful manner. Its recommendations are in many cases adopted by government agencies, cabinet committees or select committees when they are considering policy and legislative proposals. In every case the Commissioner must have due regard for competing interests to be balanced with privacy.

Compliance

The Commissioner receives, investigates and seeks to settle complaints about an interference with individual privacy. Where there appears to have been an interference with privacy and the case has not settled, the Commissioner can refer the matter to the Human Rights Review Tribunal. The Commissioner is also empowered to undertake inquiries into general matters where the privacy of the individual may be affected.

On occasion, the Commissioner is involved in privacy-related litigation.

Education and publicity

The Office promotes an understanding of the information privacy principles and the wide-ranging nature of privacy issues. Communications activities include an 0800 enquiries helpline (handling some 6,000+ calls per year), the website, training workshops and seminars, publications, speeches and responses to media enquiries.

Information matching programmes

The Office monitors the growing number of government information matching programmes, under Part 10 of the Privacy Act. Currently, there are 46 active information matching programmes being monitored.

Codes of practice

The Privacy Commissioner may issue codes of practice. Codes can modify the information privacy principles or prescribe how information privacy principles are to be applied or complied with, in a particular industry or context. Significant codes include the Health Information Privacy Code 1994, the Telecommunications Information Privacy Code 2003 and the Credit Reporting Privacy Code 2004.

International

Privacy can be significantly affected by developments beyond our borders such as new technologies, methods of data processing and standard setting. Personal data moves across national borders and requires internationally based solutions to protect privacy rights. Rules implemented by our trading partners can require New Zealand to have strong privacy laws if we are to receive data about their citizens.

The Privacy Commissioner actively works and shares knowledge with counterparts overseas and others involved in protecting privacy. The Office is particularly active in the Asia-Pacific region.

Other statutory functions of the Privacy Commissioner

These include, for example:

- monitoring compliance with the public register privacy principles;
- undertaking research into, and monitoring developments in, data processing and computer technology to ensure that any adverse effects of such developments on the privacy of individuals are minimised;
- reporting on any matters that require government attention, including the need for and desirability of taking legislative, administrative or other action to give protection or better protection to the privacy of the individual.

The Operating Environment

The potential for intrusions into the privacy of individuals is rising rapidly, mainly because of developments and convergences in information and communications technology. These provide an increasing power to collect, use and store personal information from a widening range of sources. Both government and business have an interest in, and the means to acquire, manipulate and use personal information on a very large scale.

There can be tensions between what is technically possible and the legal, or other, protections that exist to safeguard individual privacy. Privacy invasive technologies and the power of government and business to collect information on individuals are raising public awareness of the need for protection against misuse. Independent surveys show an increasing public concern about privacy issues.

Personal information is the new currency of business and government and is managed on an increasingly large scale. In this environment citizen and customer trust can be eroded by poor information handling processes. Lack of care may lead to major breaches of privacy, ranging from accidental unauthorised disclosure to data theft and misuse. Recent large scale data losses in the United Kingdom, and elsewhere, highlight the importance of sound information handling practices. On the other hand, the protection of personal information will build trust, and be a business enabler, particularly if the information management processes are transparent.

The internet and access to it has grown exponentially since the Privacy Act was passed in 1993. Recent survey results show that approximately 81% of the New Zealand population use the internet. This technology and communications revolution places new demands upon the Office in its monitoring, policy and education functions.

The steady growth in the number of new government information matching programmes will continue. Increases in matching activity are also expected to occur through expansions to existing programmes.

Science developments have accelerated, and often affect privacy. Advances in genetics are an obvious example. Pressure to incorporate such advances in our everyday lives may be driven by commercial imperatives.

Privacy is a global issue. Globalisation, international trade – especially electronic commerce – and overseas ownership of firms operating in New Zealand all have privacy implications. The spread of global anti-terrorism measures imposed by governments also have the potential to erode privacy.

STRATEGIC DIRECTION

Our challenge

It is easy to take privacy for granted in a democracy that has been relatively free of the serious human rights abuses experienced elsewhere. The race to develop and take advantage of new science and technology is an exciting one, and we are lucky to be part of it. We should also recognise that there are great opportunities to protect personal information and privacy, and enhance human rights, as part of those developments. We can only hope to do this by working cooperatively with science and technology developers, while at the same time raising public awareness, identifying threats to individual information and empowering people to protect their own privacy and personal information.

Drivers

The Privacy Commissioner must respond to the rapid advances in technology and the impact they have on individual privacy. Opinion surveys highlight individual concern about the manner in which personal information is collected, managed and distributed by business and government.

In order to be a watchdog on privacy invasions and potential threats to privacy, and to advise and comment effectively, the Commissioner must be seen to be independent of government, business and other interests.

Because of the dynamic nature of the privacy environment, the Office will monitor and anticipate developments. Provision of advice on privacy impacts, especially to government and its agencies, is imperative. Monitoring and advising upon technology developments will remain a major priority, given the strong and widespread impact on individual privacy through these changes.

Rapid technological change places increased pressures on personal information handling practices. Advances in technology outstrip conventional information handling techniques; for example, the increased use of biometrics for identity verification across business and government, and the use of DNA in identity, health information and other areas. The effectiveness of legislation or other measures must be maintained to provide up-to-date protection for individuals.

Government Priorities and Justice Sector Outcomes

The Office of the Privacy Commissioner is an independent Crown entity (Part 3 of Schedule 1, Crown Entities Act). This independence supports New Zealand's reputation for sound governance and international standards, while allowing it to contribute to Government priorities and Justice Sector outcomes.

The work of the Office strongly supports Government priorities of Economic Transformation and Families - Young and Old. Further, the work of the Privacy Commissioner supports the broader Justice Sector outcome of a Safe and Just Society, contributing to a Trusted Justice System and International Connectedness. In receiving and investigating complaints against public agencies, and independently monitoring government information matching programmes, the work of the Office further contributes to the Justice Sector outcome of Effective Constitutional Arrangements.

Economic Transformation is supported through robust and effective privacy protections and standards. The outputs of the Office facilitate government and business to meet the public's expectations of how their personal information is managed, while removing international barriers to the exchange of personal information between countries.

The Privacy Commissioner's role is changing, with a stronger emphasis on good personal information practices as an enabler to reap the business and economic benefits of science and technology. New Zealand business success requires trust by individuals in the accuracy, security and purpose for which personal information is collected and maintained and the manner in which it is used by business and government.

The facilitation of trade through the interchange of personal information and data is an important vehicle through which businesses can become more competitive. Currently New Zealand is at an increasing competitive disadvantage in the growing world of cross-border trade in technology and services. Changes to the Privacy Act are needed to bring our law into line with European Union (EU) requirements, a necessary step to facilitate business opportunities with that important trading bloc and enhance our economic capability. In our own region, APEC is also actively advancing a privacy agenda and New Zealand needs to engage to ensure the outcomes are positive for citizens, consumers and

businesses.

The Privacy Commissioner maintains close working relationships with other international jurisdictions and through these relationships facilitates and influences an understanding of the needs of New Zealand business, government and individuals.

OPERATING INTENTIONS

We shall work towards a modern New Zealand which;

- recognises the individual and societal value in protecting privacy
- reflects excellence in personal information handling by government and business
- recognises and reacts to the changing privacy demands of the electronic age.

We will implement four intermediate outcomes which support the high level operating intentions of the Office. They are as follows:

i. Improved privacy awareness in the community

There is considerable work to be done in further developing public awareness, so that there is a more equal balance between the agencies with huge power to gather and manipulate information, and the individuals whose information makes up these databases. A balanced public debate is desirable. The Office needs to develop its understanding of the extent of privacy awareness across all groups in the community and develop effective means to empower individuals to protect their privacy.

Key impacts sought

- Wider public access to, and greater use of, privacy information and resources.
- Increased awareness of the benefits of good information handling among individuals.

Activities

Key initiatives planned are to:

- Deliver effective external communications
- Publish additional resources, particularly web based publications and case notes including those focusing on technology, privacy and business needs
- Target key privacy concerns and interest groups
- Engage with a wide range of individuals and agencies
- Undertake consultation and research as appropriate
- Promote a wide and informed debate on privacy issues
- Develop education initiatives to improve privacy awareness in the community
- Undertake an independent public opinion survey.

Monitoring

Impacts will be monitored by analysing enquiries and complaints, feedback received from the public, conducting surveys to determine public awareness, and measuring website use.

ii. Improved privacy standards and practice in government and business

Agencies vary in the extent to which they consider and address the privacy impacts of their actions, in their handling of personal information. Opinion surveys indicate that New Zealanders are concerned about the misuse of personal information and invasion of individual privacy by technology. Unease exists around privacy intrusions in areas such as employment, finance, telecommunications and health.

The Commissioner acts as a watchdog to respond to privacy concerns and to encourage responsible stewardship of personal information. The Office encourages government and business to find ways to achieve their objectives while respecting the personal privacy of individuals.

Key impacts sought

- Government and business are assisted to develop practices that respect privacy.
- The public's trust that government and business will handle personal information fairly is enhanced.
- Legislation, policy and practices respect the privacy principles.
- Data matching programmes are assessed and monitored.
- New Zealand business harnesses the benefits of technology while better understanding privacy risks and solutions.

Activities

Key initiatives planned are to:

- Monitor and advise on the privacy impacts of proposed legislation and policy initiatives
- Contribute to and help guide e-government initiatives
- Scope potential solutions to the privacy impacts of inter-agency sharing of personal information
- Provide policy advice on key privacy matters in relation to health information policy development
- Contribute to and as necessary assist the Law Commission Review of Privacy
- Actively support the development of a network of privacy officers
- Monitor and report on government data matching programmes
- Develop and improve guidance materials for government and business
- Enhance guidance resources to assist agencies conducting information matching
- Promote better practice with public CCTV systems
- Participate in international privacy forums to identify global privacy issues and threats and promote best practice, standard setting and co-operation amongst international enforcement authorities.

Monitoring

The quality of advice to government agencies will be tested through informal feedback mechanisms. Statistics for legal and policy work will be used to provide comparative analysis with previous years. Independent public opinion surveys will provide a measure of the public's perception of information handling by business and government.

iii. Individuals are equipped to resolve their privacy concerns

The Privacy Act encourages awareness and self-resolution of problems for individuals. An informal non-punitive environment encourages mediation, conciliation, settlement negotiations and overall positive outcomes. Nevertheless, individuals need access to a low cost way to challenge how their information is being used and to obtain any necessary redress.

Key impacts sought

- People and groups are empowered to take ownership of and self-resolve privacy issues.
- Complaints and enquiries are handled in a fair and timely manner.

Activities

The key initiatives planned include:

- Managing complaints investigations so that 80 - 90% of complaints are completed within 12 months of receipt
- Providing the website and other resources to help individuals and agencies to avoid problems in the handling of personal information and to resolve complaints where they arise
- Ensuring the website provides an easily navigable source of plain English information on privacy issues for individuals
- Providing an enquiries service and 0800 helpline on privacy matters
- Identifying opportunities for cross-border co-operation in the resolution of complaints involving a cross-border element.

Monitoring

- Monthly performance statistics will track complaints resolution – including time to complete.
- Annual surveys of complainant and respondent satisfaction will be undertaken.
- The quality of the complaints service will be regularly and independently audited.
- Website use will be monitored and content regularly updated.
- The enquiries function will be reported on and audited.

iv. New Zealanders' privacy is promoted through engagement at an international level

In the growing world of e-commerce and cross-border trade, such as offshore processing of data, New Zealand needs to meet the data protection standards of our trading partners to better facilitate and protect our trading relationships.

New Zealanders want their personal information protected wherever it travels. The Office of the Privacy Commissioner can play a useful part through effective engagement with others involved in protecting privacy in other countries and at an international level in researching privacy risks and regulatory strategies, standard setting and enforcement co-operation.

Key impacts sought

- New Zealand privacy legislation and practice accords with international standards.
- The Privacy Act is amended to harmonise with EU requirements for transborder transfers of personal data, in order to strengthen New Zealand's case for "white list" status under the EU Directive on the Protection of Individuals in Relation to the Processing of Personal Data and on the Free Movement of Such Data.

Activities

The key initiatives planned are to:

- Provide advice to Parliament and the Minister on the merit of legislative amendment to the Privacy Act to meet EU standards for data processing
- Monitor international privacy activities, codes and standards for their impact upon New Zealand's trade and investment opportunities
- Make information relating to New Zealand's privacy standards known to overseas regulators
- Enhance, or, where they do not yet exist, create, mechanisms to promote co-operation with overseas privacy regulators and to facilitate the exchange of information across jurisdictions
- Contribute to ongoing APEC and OECD initiatives to enhance cross-border co-operation in privacy enforcement.

Monitoring

Amendments to the Privacy Act will be in effect and reports to the Minister will contain monitoring information on international developments.

MANAGING IN A CHANGEABLE OPERATING ENVIRONMENT

RISKS

The Office has identified four major risks and responses to address those risks:

RISK TYPE	RESPONSE
<p>Credibility: The risk that the Office loses influence with government, business and the media. The Office loses relevance</p>	<p>Ensuring statutory obligations are met as well as information and advisory responsibilities</p> <p>Ensuring that the Office of the Privacy Commissioner 's position and advice on issues is evidence based – through the use of reliable information and robust research</p> <p>Ensuring that the Office remains abreast of international privacy developments</p>
<p>Demand and expectations: The risk that the Office cannot meet the level of complaints, enquiries and demand for information arising from increased awareness</p>	<p>Self resolution measures and tools are in place</p> <p>Current priority systems are maintained and developed further if necessary</p> <p>Ensure that information is disseminated to reach a wide audience</p>
<p>International standards: The risk that New Zealand fails to meet international privacy requirements</p>	<p>Continuing participation in international privacy networks</p> <p>Promoting legislation to reflect these standards</p>
<p>Staff skills: The risk that key skill capabilities are not available for the Commissioner's work. Staff knowledge is lost</p>	<p>Planning recruitment and retention to ensure that the required skills are developed and maintained</p> <p>Ensuring staff are supported with professional development and performance management systems</p> <p>Ensuring opportunities exist for gaining wider experience and career development</p>

Environmental Scanning

The Privacy Commissioner commissions independent research to assess individual concerns, awareness and developing trends in privacy within New Zealand. These regular surveys allow monitoring of changes over time.

In addition, the Office will implement a pilot programme to assess its performance against similar jurisdictions in the Asia-Pacific region.

The Office participates in many public fora and speaking engagements, develops education programmes from which information and feedback is received and maintains close links with privacy officer interest groups in the public and private sectors.

ASSESSING ORGANISATIONAL HEALTH AND CAPABILITY

People

The Office requires a mix of a high level of legal, investigative, technology, policy and communication skills. As a small office it is highly dependent on developing and retaining staff skills and knowledge. The loss of key staff would result in a significant knowledge deficit which would not be easily regained. Therefore a strategic priority is the enhancement of staff skills, knowledge and experience. The Office employs contract staff for specialist areas as required.

Systems

Systems include electronic records and a document management system to enhance our capabilities to survey, monitor, and track processes and practices across all work areas within the Office.

Relationships

The Privacy Commissioner actively works with the state sector, business, civil society, academics and the media. The Office is an active participant in international privacy networks.

The Office works with the State Services Commission on privacy issues and policies in the e-government initiative. A policy adviser position has been funded by the Ministry of Health to enable the Office to provide advice on health privacy issues.

Financial

The Privacy Commissioner has delivered services with little or no change in baseline funding over the past three years. We manage within these financial constraints, and focus on maintaining the quantity and quality of the services delivered.

We have budgeted for a further deficit this year, as we did in 2007/08. The pressures of increasing demand and technology impacts on privacy make the current financial baseline unsustainable for the period post the 2008/09 financial year.

Equal employment opportunities and good employer statement

The Office has an EEO policy and is an equal opportunities employer in its recruitment, human resources and staff development practices. The Office has documented human resource policies and regularly monitors staff morale as part of management reporting. Exit interviews are carried out as part of continuously improving employment policies.

The Office of the Privacy Commissioner has a personnel policy containing provisions for the fair and proper treatment of employees in all aspects of their employment.

We review our workplace profile and report its representativeness through the production of the Good Employer Report. We consult with staff on issues of concern and review existing policies, practices, documents and systems in all areas of business to ensure equal opportunities in recruitment, appointment, development, promotion and remuneration.

We will incorporate the remaining Key Employment Elements in 2008/09 and report on them in the Annual Report.

Service Performance

Outputs

1. Policy

Provide advice on the privacy impact of proposed legislation and other significant proposals.

Monitor and advise on international developments, new technologies and other issues affecting privacy.

Assess proposals for information matching, monitor and report on authorised information matching programmes and review statutory authorities for information matching.

Quantity

- Contribute to the Law Commission's review of privacy.
- Review of the Privacy Act:
 - Assist the Ministry of Justice in pursuing a finding from the European Union that New Zealand law offers an "adequate" standard of data protection;
 - Support the Ministry of Justice on the review of the Act and proposed legislative change process.
- Issue and keep current codes of practice.
- Provide practical advice to departments on privacy issues and fair information practices arising in proposed legislation and in administrative proposals.
- Provide specialised assistance to government departments in accordance with agreed memoranda of understanding.
- Provide assistance to improve whole of government compliance with information matching controls.
- Contribute to international initiatives to facilitate cross-border co-operation in privacy standard setting and enforcement.

Quality

- All proposals for codes of practice will be the subject of discussion with stakeholders and a public submission process which includes a clear statement of purpose.
- All issued codes are referred to the Regulations Review Committee of the House of Representatives.

- Assistance provided to government agencies which presents a clear, concise and logical argument, with assumptions made explicit and supported by facts.
- Respond to feedback obtained from recipients of advice.

Timeliness

- Codes of practice meet the agreed timelines for release and implementation.
- Give advice within a time span that will enable it to be useful to the recipient or within agreed timeframes.

2. Communications

Implement our “outreach” programme across all activities of the Office to support and promote:

- awareness and understanding of and compliance with the Privacy Act, and
- privacy as a human right and develop an awareness of privacy issues.

Quantity

- Organise New Zealand Privacy Awareness Week as part of the Asia-Pacific Privacy Awareness Week.
- Undertake speaking engagements.
- Respond to media enquiries.
- Provide assistance to promote better privacy practice in the development of policy and legislation and administrative practices by government agencies.
- Contribute to Law Commission Privacy Review.
- Participate in international fora.
- Support, where appropriate, networking by agency privacy officers, to develop and improve their effectiveness.
- Undertake a programme of education workshops to promote awareness and understanding of and compliance with the Privacy Act.

- Provide a free enquiries service including 0800 helpline and website access to information, supporting self-resolution of complaints.
- Maintain an effective website and other publications to assist stakeholders to promote better privacy practice.
- Commission an independent survey of public opinion to measure privacy awareness and the range of attitudes to privacy within the community.

Activities

	Estimation
Education workshops	60
Presentations at conferences / seminars	10
Projected number of enquiries received and answered	6,000
Case notes produced	20
Information matching workshops	1
Technology and Policy forums	6

Quality

- Meet internal professional standards.
- Act on feedback obtained from recipients of advice.
- Evaluations show that the expectations of 90% of attendees at workshops were either met or exceeded for quality of presentation and materials.
- Publications and information are legally accurate.
- Case notes conform to regional standards adopted by the Asia Pacific Privacy Authorities (APPA).
- Meetings held with or presentations made to at least 10 significant privacy interest groups.
- Reliable and relevant information is placed on the website.
- Enquiries are answered by appropriately trained professional staff.

Timeliness

- Workshop timetables published on the website.
- Current information is placed on the website within a month of being made available.
- Response times to enquiries meet internal standards.

3. Compliance

- Handle complaints of interference with privacy.
- Enhance cooperation between privacy regulators internationally.
- Undertake Commissioner initiated investigations (as required).
- Monitor active information matching programmes.

Quantity

	Estimation
Number of complaints received	600
Number of current complaints processed to completion or settled or discontinued	600
Projected number of active information matching programmes monitored	46

Quality

- Complainants' and respondents' satisfaction with the complaints handling process rated as "satisfactory" or better in 80% of responses to a survey of complaints received and closed in the preceding period.
- When a Human Rights Review Tribunal case is concluded, the outcome will be reviewed against the work of the Office with the findings reported to the Privacy Commissioner.
- External review is conducted of a sample of complaints investigations for their standard of the legal analysis, correctness of the legal conclusions, soundness of the investigative procedure and timeliness.

- Referrals to the Director of Proceedings meet expected standards of evidential sufficiency and public interest in all cases.
- Reports on authorised information matching programmes to be published will be submitted to relevant departments for comment before publication.

Timeliness

- 80-90% of complaints are completed, settled or discontinued within 12 months of receipt.
- A report on all authorised information matching programmes will be provided annually.

Financial forecast statements

Statements of forecast financial performance, position and cash flows for the year ending 30 June 2009

OFFICE OF THE PRIVACY COMMISSIONER STATEMENT OF FINANCIAL PERFORMANCE BUDGET FOR YEAR ENDED 30 JUNE 2009

2007/2008		2008/2009
Budget		Budget
\$		\$
	INCOME	
3,109,000	Operating Grant	3,148,000
36,000	Education	36,000
52,000	Interest Received	60,000
255,556	Other Income	278,656
3,452,556	TOTAL INCOME	3,522,656
	EXPENDITURE	
2,437,567	Personnel	2,546,336
15,000	Audit Fees	20,000
156,000	Depreciation	168,000
360,000	Rental	324,435
445,300	Operating Costs	434,100
49,300	Marketing/Newsletter	72,000
3,463,167	TOTAL EXPENDITURE	3,564,871
10,611	EXCESS EXPENSES OVER INCOME	42,215

OFFICE OF THE PRIVACY COMMISSIONER
STATEMENT OF FINANCIAL POSITION
BUDGET FOR YEAR ENDED 30 JUNE 2009

Forecast 2008		Budget 2009
	CURRENT ASSETS	
450	Cash on Hand	450
46,998	National Bank – Cheque	61,595
500,000	National Bank - Deposit	600,000
-	Debtors	-
5,271	Inventory	5,271
-	GST Receivable	-
8,129	Prepayments	8,129
560,848		659,131
595,735	Fixed Assets	463,735
1,156,583		1,122,866
	CURRENT LIABILITIES	
50,000	Sundry Creditors	50,000
139,245	GST Payable	161,257
44,000	Accruals	44,000
58,000	Employee Entitlements	58,000
288,245	Total Current Liabilities	296,743
868,338	NET ASSETS	826,123
868,338	Accumulated Funds	826,123
868,338	PUBLIC EQUITY	826,123

OFFICE OF THE PRIVACY COMMISSIONER
 STATEMENT OF CASH FLOWS
 BUDGET FOR YEAR ENDED 30 JUNE 2009

	Budget 2009
	\$
Cash Flows from Operating Activities	
Cash was provided from:	
Operating Grant	3,148,000
Other Income	314,556
Interest	60,000
	<u>3,522,556</u>
Cash was applied to:	
Payments to Suppliers	850,435
Payments to Employees	2,546,336
Payments of GST	(24,812)
	<u>3,371,959</u>
Net Cash Flows applied to Operating Activities	<u>150,597</u>
Cash Flows from Investing Activities	
Cash was provided from:	
Sale of Fixed Assets	-
	<u>-</u>
Cash was applied to:	
Purchase of Fixed Assets	36,000
	<u>36,000</u>
Net Cash Flows applied to Investing Activities	<u>36,000</u>
Net increase (decrease) in cash held	114,597
Cash brought forward	547,448
	<u>662,045</u>
Closing cash carried forward	<u>662,045</u>
Cash made up of:	
Cash on Hand	450
National Bank	61,595
National Bank – Deposit	600,000
	<u>662,045</u>

RECONCILIATION OF CASH FLOWS FROM OPERATING ACTIVITIES

Excess Expenditure over Income	(42,215)
Non-Cash Item	
Depreciation	168,000
Profit on sale of Fixed Assets	-
Movements in Working Capital	
Increase (Decrease) in Creditors	-
Increase (Decrease) in Accruals	-
(Increase) Decrease in GST	24,812
Increase (Decrease) in Employee Provision	-
Increase (Decrease) in Inventory	-
(Increase) Decrease in Prepayments	-
(Increase) Decrease in Debtors	-
	150,597

Statement of Forecast Service Performance

The Privacy Commissioner has committed to provide three output classes in 2008/09 that meet the requirements of the Minister of Justice in terms of their description, quantity, timeliness and costs.

Output operating statements: 2008/09

Departmental Output Class Description	Revenue	REVENUE		EXPENSES	SURPLUS
	Crown	Revenue Other	Capital Contribution	Total Expenses	Surplus / (Deficit)
	\$000	\$000	\$000	\$000	\$000
· Privacy Policy	1,018	219	0	1,255	(18)
· Communications	695	103	0	832	(34)
· Compliance	1,435	53	0	1,478	10
TOTAL DEPARTMENTAL OUTPUT CLASSES	3,148	375	0	3,565	(42)

STATEMENT OF ACCOUNTING POLICIES

Reporting entity

These are the financial statements of the Privacy Commissioner, a Crown entity in terms of the Public Finance Act 1989.

These financial statements have been prepared in accordance with the Public Finance Act 1989.

In addition, the Privacy Commissioner has reported the funding administered on behalf of the Crown as notes to the financial statements.

Measurement base

The financial statements have been prepared on an historical cost basis.

Accounting policies

The following particular accounting policies which materially affect the measurement of financial performance and financial position have been applied.

Budget figures

The budget figures are those approved by the Privacy Commissioner at the beginning of the financial year.

The budget figures have been prepared in accordance with generally accepted accounting practice and are consistent with the accounting policies adopted by the Privacy Commissioner for the preparation of the financial statements.

Revenue

The Privacy Commissioner derives revenue through the provision of outputs to the Crown, for services to third parties and income from its investments. Such revenue is recognised when earned and is reported in the financial period to which it relates.

Goods and Services Tax (GST)

All items in the financial statements are exclusive of GST, with the exception of accounts receivable and accounts payable which are stated with GST included. Where GST is irrecoverable as an input tax, then it is recognised as part of the related asset or expense.

Taxation

The Privacy Commissioner is a public authority in terms of the Income Tax Act 1994 and consequently is exempt from income tax.

Accounts receivable

Accounts receivable are stated at their expected realisable value after providing for doubtful and uncollectable debts.

Property Plant and Equipment

All fixed assets, or groups of assets forming part of a network which are material in aggregate are capitalised and recorded at cost. Any write-down of an item to its recoverable amount is recognised in the statement of financial performance.

Depreciation

Depreciation is provided on a straight line basis on all fixed assets, at a rate which will write off the cost (or valuation) of the assets to their estimated residual value over their useful lives.

The useful lives and associated depreciation rates of major classes of assets have been estimated as follows:

Furniture and fittings	5 years
Computer equipment	4 years
Office equipment	5 years

Employee Entitlements

Provision is made in respect of the Privacy Commissioner's liability for annual, long service and retirement leave. Annual leave and other entitlements that are expected to be settled within 12 months of reporting date, are measured at nominal values on an actual entitlement basis at current rates of pay.

Entitlements that are payable beyond 12 months, such as long service leave and retirement leave, have been calculated on an actuarial basis based on the present value of expected future entitlements.

Related Parties

The Privacy Commissioner is a wholly owned entity of the Crown. The Government significantly influences the role of the Privacy Commissioner as well as being its major source of revenue.

The Privacy Commissioner has entered into a number of transactions with government departments, Crown agencies and state-owned enterprises on an arm's length basis. Where those parties are acting in the course of their normal dealings with the Privacy Commissioner, related party disclosures have not been made for transactions of this nature.

There were no other related party transactions.

Leases

Operating leases

Leases where the lessor effectively retains substantially all the risks and benefits of ownership of the leased items are classified as operating leases. Operating lease expenses are recognised on a systematic basis over the period of the lease.

Financial instruments

The Privacy Commissioner is party to financial instruments as part of its normal operations. These financial instruments include bank accounts, short-term deposits, debtors, and creditors. All financial instruments are recognised

in the statement of financial position and all revenues and expenses in relation to financial instruments are recognised in the statement of financial performance.

Statement of cash flows

Cash means cash balances on hand, held in bank accounts, demand deposits and other highly liquid investments in which the Privacy Commissioner invests as part of its day-to-day cash management.

Operating activities include all activities other than investing and financing activities. The cash inflows include all receipts from the sale of goods and services and other sources of revenue that support the Privacy Commissioner’s operating activities. Cash outflows include payments made to employees, suppliers and for taxes.

Investing activities are those activities relating to the acquisition and disposal of current and non-current securities and any other non-current assets.

Accumulated reserves

The Privacy Commissioner is able to accumulate reserves from previous years which provide capability to meet capital expenses and unbudgeted one-off expenses. Accumulated reserves are an estimate only of projected reserves to be carried over from the 2007/08 financial year and are subject to change following the audit of the year end accounts.

Accumulated reserves in 2008/09 will be used for:

	\$000
Appointment of Communications Adviser as part of Communications Pilot Project (Year 2 of 2 year project)	100
Provision for capital works for relocation of Wellington office late 2009	250
Providing for unexpected impacts throughout the year	100
Contingency to meet projected deficit in 2008/09	50

Transition to New Zealand International Financial Reporting Standards

The Privacy Commissioner adopted NZIFRS and report for the first time under NZIFRS for the year ended 30 June 2008. Comparative information to 30 June 2007 presented in the Financial Statements will be restated to meet the requirements of the new standards and the financial impact of adoption (which may be material) will be disclosed. The Privacy Commissioner does not expect difficulties with the adoption of NZIFRS.

Changes in accounting policies

There have been no changes in accounting policies, including cost-allocation accounting policies. All policies have been applied on bases consistent with those used in the previous period.

