



PRIVACY MANAGEMENT PLAN

by

Corporate Services

Sydney Harbour Foreshore Authority

Document Control

Approved by:	Corporate Governance Committee
Date of Approval:	July 2009
Review Cycle:	Annual
Review Date:	July 2010
Division Originating:	Corporate Services
Officer Responsible:	Legal Services Manager

Table Of Contents

1	CEO'S STATEMENT	4
2	GENERAL	5
2.1	OVERVIEW.....	5
2.2	PURPOSE.....	5
2.3	RESPONSIBILITIES.....	5
2.4	DOCUMENT HISTORY	5
2.5	POLICY STATEMENT.....	5
3	INTRODUCTION.....	6
4	REQUIREMENTS OF THE PLAN.....	6
4.1	WHAT IS PERSONAL INFORMATION?.....	6
4.2	ACCURACY OF PERSONAL INFORMATION.....	7
4.3	LIMITS ON THE USE OF PERSONAL INFORMATION	7
4.4	THE INFORMATION PROTECTION PRINCIPLES (IPPs)	7
4.5	PRIVACY CODES OF PRACTICE	9
4.6	PUBLIC REGISTERS.....	9
4.7	HEALTH PRIVACY PRINCIPLES	9
5	HOW THE AUTHORITY MANAGES PERSONAL INFORMATION	9
5.1	CORPORATE SERVICES	9
5.2	MARKETING AND EVENTS	10
5.3	STRATEGIC DEVELOPMENTS	11
5.4	PROPERTY AND ASSET MANAGEMENT	11
6	EXISTING POLICIES AND LAWS RELATING TO INFORMATION	12
7	IMPLEMENTING THE PRIVACY MANAGEMENT PLAN.....	12
7.1	CLASSES OF PERSONAL INFORMATION.....	12
7.2	HEALTH INFORMATION	14
8	COMPLIANCE WITH THE PRIVACY IPPS	15
8.1	COLLECTION OF INFORMATION.....	15
8.2	STORAGE	15
8.3	STORING INFORMATION - CORPORATE SERVICES	15
8.4	STORING INFORMATION – MARKETING AND EVENTS	15
8.5	STORING INFORMATION – STRATEGIC DEVELOPMENTS	16
8.6	STORING INFORMATION – PROPERTY AND ASSET MANAGEMENT.....	16
8.7	NOTIFICATION, ACCESS AND CORRECTION.....	16
8.8	DISCLOSURE	16
8.9	PROTECTION OF PERSONAL INFORMATION	17
8.10	COMPLIANCE WITH THE PUBLIC REGISTER PROVISIONS	17
9	THE INTERNAL REVIEW PROCESS.....	18
9.1	WHO CAN CALL FOR A REVIEW?	18
9.2	WHAT ACTIONS MIGHT PRECIPITATE A REVIEW?	18
9.3	WHO DEALS WITH INTERNAL REVIEWS?	18
9.4	WHAT THE AUTHORITY MUST DO.....	18
9.5	HOW THE AUTHORITY RESPONDS TO A REVIEW.....	18
9.6	WHAT HAPPENS IF A PERSON IS NOT SATISFIED WITH AN INTERNAL REVIEW?	19
10	DISSEMINATION OF POLICIES AND PRACTICES	19
11	CODES OF PRACTICE	19
12	DISCLOSURE OF PERSONAL INFORMATION OUTSIDE NSW	19
13	CONTACTS/REFERENCES	21
13.1	CONTACTS	21
13.2	RELEVANT LEGISLATION.....	21
13.3	OTHER RELEVANT POLICIES/PUBLICATIONS	21

14	APPENDICES	21
14.1	APPENDIX A – DEFINITIONS.....	22
14.2	APPENDIX B – INFORMATION PROTECTION PRINCIPLES IN APPLICATION	23
14.3	APPENDIX C – APPLICATION FOR REVIEW OF CONDUCT.....	26
14.4	APPENDIX D –REVIEW OF CONDUCT – AUTHORITY CHECKLIST	27

1 CEO'S STATEMENT

The Sydney Harbour Foreshore Authority presents the Privacy Management Plan in response to the Privacy and Personal Information Act 1998. The Authority collects and maintains a limited amount of personal information relating to its staff, tenants and, to a lesser extent, its service providers. The Authority is committed to applying the statutory requirements of the Act and welcomes the guidelines provided by the Information Protection Principles. staff as well as tenants and stakeholders

The Authority's Privacy Management Plan is made available to staff on the Intranet and is available to members of the public on request. The protection of personal information remains a process of ongoing diligence for the Authority. All staff are required to complete the e-learning module on privacy to ensure that they have a knowledge of the principles involved. This Plan will be periodically reviewed and updated to reflect any changes to the legislation and to incorporate improvements to practices or principles.

Robert Domm
Chief Executive Officer

2 GENERAL

2.1 OVERVIEW

This plan was developed to describe Sydney Harbour Foreshore Authority's statutory obligations when gathering, handling, disclosing and storing personal information belonging to staff, clients, tenants, contractors, members of the public, etc.

2.2 PURPOSE

The Privacy Management Plan has been developed in accordance with the *Privacy and Personal Information Protection Act 1998* (the Act). The Act is based on 12 Information Protection Principles which establish acceptable standards for using personal information in an open and accountable manner. This plan was also developed in accordance with the *Health Records and Information Privacy Act 2002* outlining how health information must be collected, stored, used and disclosed.

2.3 RESPONSIBILITIES

All staff are required to understand their obligations under the Privacy Management Plan. In order to achieve this, all staff are required to complete the e-learning module on privacy to ensure that they have a knowledge of the principles involved.

2.4 DOCUMENT HISTORY

Date	Author	Modifications
June 2009	A/Legal Services Manager	Review, amendment to reflect organisational structure, put into new template
October 2008	Corporate Secretary	Review, minor amendments to reflect organisational structure, Policy Template update.
September 2006	Manager Corporate Governance	Created original document.

2.5 POLICY STATEMENT

This plan gives staff an understanding of the definition of "personal information" and how the Authority manages the access, storage and disclosure of this information. The principles underpinning the *Privacy and Personal Information Protection Act 1998* and *Health Records and Information Privacy Act 2002* are discussed in detail so that staff gain a deep understanding of their statutory obligations when handling personal information in their roles as public servants.

The process for reviewing complaints about the handling of personal information is also discussed in this plan.

3 INTRODUCTION

The *Privacy and Personal Information Protection Act 1998* (the Act) aims to protect the privacy of individuals from the inappropriate collection, storage, use and disclosure of personal information by NSW public sector agencies. The Act is based on **12 Information Protection Principles** which establish acceptable standards for using personal information in an open and accountable manner. Sydney Harbour Foreshore Authority is a public sector agency for the purposes of the Act as it is a statutory body representing the Crown.

Under the Act, individuals have a right to make a complaint about the possible misuse of their personal information. The Act requires agencies to establish a Privacy Management Plan to document how the agency currently complies or what the agency proposes to do to comply with the new legislation.

The *Health Records and Information Privacy Act 2002* contains **15 health privacy principles** outlining how health information must be collected, stored, used and disclosed. This policy addresses these principles.

4 REQUIREMENTS OF THE PLAN

This section outlines and summarises the legal requirements of the *Privacy and Personal Information Protection Act 1998* to ensure that staff and clients better understand the law underpinning this plan.

4.1 WHAT IS PERSONAL INFORMATION?

Under the Act, personal information is any information or opinion that relates to an identifiable person. This covers both paper and electronic files whether or not recorded in a material form. The person does not have to be clearly identified by the information for it to be described as “personal”. Personal information is information about an individual whose identity is apparent or can reasonably be ascertained, so that it could be information that identifies a person by connection, for example; “the owner of Unit 17” could allow the owner to be identified through Electoral Rolls or Rate Records.

Although the definition of personal information is very broad, the Act also excludes certain types of information. The information excluded, as might relate to the Authority, is information including that which is:

- contained in a publicly available publication
- about an individual’s suitability for public sector employment
- about people who have been dead for more than 30 years.

Personal information is held by a public sector agency if:

- the agency is in possession or control of the information
- the information is in the possession or control of a person employed by or engaged by the agency in the course of such employment or engagement, or
- the information is contained in a State record in respect of which the agency is responsible under the *State Records Act 1998*.

However, personal information is not collected by a public sector agency if the receipt of the information by the agency is unsolicited.

4.2 ACCURACY OF PERSONAL INFORMATION

An agency holding personal information must not use the information without taking reasonable steps to ensure that, having regard to the purpose for which the information is proposed to be used, that it is relevant, accurate, up-to-date, complete and not misleading.

4.3 LIMITS ON THE USE OF PERSONAL INFORMATION

An agency that holds personal information must not use the information for a purpose other than that for which it was collected unless:

- the individual to whom the information relates has consented to the use of the information for that other purpose, or
- the other purpose for which the information is used is directly related to the purpose for which the information was collected, or
- the use of the information for that other purpose is necessary to prevent or lessen a serious and imminent threat to the life or health of the individual or of another person

4.4 THE INFORMATION PROTECTION PRINCIPLES (IPPs)

The IPPs are the key to how the Act is to be complied with. A list of the IPPs with a plain English explanation follows. The section number in brackets refers to the appropriate section of the Act. Further information on the IPPs are found in the *Guidance for the Public Sector factsheet* which should be read in conjunction with this document. A copy of the factsheet is at Appendix E.

4.4.1 Principle 1 – (Section 8) Collection of personal information for lawful purposes

The Authority must only collect information that is directly related to its activities or functions. This principle limits the amount of information the Authority is allowed to collect.

4.4.2 Principle 2 – (Section 9) Collection of personal information directly from the individual

It is a requirement that personal information be collected directly from the person to whom it relates. An individual can authorise someone else to provide information on their behalf.

4.4.3 Principle 3 – (Section 10) Requirements when collecting personal information

The Authority must inform an individual that:

- information is being collected
- the purpose for which the information is being collected, and
- the intended recipients of the information.
- It must also state whether the information is required by law or is voluntary; their right to review and correct the information, together with the name and address of the Authority.

4.4.4 Principle 4 – (Section 11) Other requirements relating to collection of personal information

The Authority must take reasonable steps to ensure that the personal information it collects is accurate, up-to-date and complete. The Authority cannot unreasonably intrude on the personal affairs of the individual to whom the information relates.

4.4.5 Principle 5 – (Section 12) Retention and security of personal information

The information collected by the Authority must not be kept longer than is needed. When the information is no longer required it must be disposed of securely. The Authority must take all reasonable steps to prevent unauthorised use of the information by means of secure storage and other appropriate controls.

4.4.6 Principle 6 – (Section 13) Information about personal information held by agencies

This principle is designed to alert people to the fact that the Authority holds personal information. This is an important principle allowing people to exercise their rights under the Act.

4.4.7 Principle 7 – (Section 14) Access to personal information held by agencies

Individuals have a right of access to their personal information held by the Authority. This principle looks at the interaction of the Act with the *Freedom of Information Act 1989*.

4.4.8 Principle 8 – (Section 15) Alteration of personal information

This principle provides a right to correct any personal information which a person believes to be incorrect or inappropriate.

4.4.9 Principle 9 – (Section 16) Agency must check accuracy of personal information before use

The Authority has an obligation to try to ensure that all personal information used is relevant and accurate.

4.4.10 Principle 10 – (Section 17) Limits on use of personal information

The Authority is limited in the uses it can make of any personal information that it collects or holds. It generally restricts use to the purpose for which the information was collected.

4.4.11 Principle 11 – (Section 18) Limits on disclosure of personal information

As a general rule, personal information should be disclosed only for purposes directly related to those for which the information was collected.

4.4.12 Principle 12 – (Section 19) Special restrictions on disclosure of personal information

There are two distinct parts to this section. The first part deals with a number of categories of sensitive information which cannot be disclosed (such as an individual's age, ethnic or religious origin, marital status, health or sexual activities).

The second part places restrictions on disclosure of personal information to persons or bodies outside New South Wales.

4.4.13 Conclusion

The Information Protection Principles provide the basic approach to information privacy protection by public sector agencies which are bound by the Act. The wide range of exceptions to strict compliance, together with the possibility of gaining an exemption by means of a privacy Code of Practice, or an order by the Privacy Commissioner under Section 41, means that they should not interfere with agencies' practical and legitimate processing requirements.

Privacy NSW's role in relation to the principles is primarily an advisory and monitoring one to ensure their effectiveness in achieving an appropriate standard of privacy protection.

4.5 PRIVACY CODES OF PRACTICE

Privacy Codes of Practice identify activities which depart from the Information Protection Principles or apply the Principles in a special way. At this stage the Authority does not intend implementing any Privacy Codes of Practice.

4.6 PUBLIC REGISTERS

The Authority maintains a public register of Development Applications affecting property under its control, the Authority also maintains a Land Register.

4.7 HEALTH PRIVACY PRINCIPLES

The *Health Records and Information Privacy Act 2002* contains 15 health privacy principles that can be grouped into seven main headings – collection, storage, access and accuracy, use, disclosure, identifiers and anonymity, and transferrals and linkage. These principles are addressed in **Section 7, Implementing the Privacy Management Plan**.

5 HOW THE AUTHORITY MANAGES PERSONAL INFORMATION

The Authority has a number of separate cost/task centres established as divisions or units. A brief description of the divisions, together with the type of personal information that they hold, follows:

5.1 CORPORATE SERVICES

This division provides budgeting, financial management, information communication technology, procurement, external relations, general administration and human resource services. The Corporate Services division also provides support for the Authority and the Board and liaises with the Minister's office and other government agencies. The division handles Freedom of Information (FOI) and Privacy requests, ensures correct corporate governance, and satisfies government agency reporting requirements.

The units within Corporate Services are:

- Finance
- External Relations (incorporating Corporate Secretary, Legal Services and Design Studio)
- Human Resources
- Information, Communication and Technology (incorporating E-Services and records)
- Procurement

5.1.1 Finance

The Finance unit deals with budgeting, accounts payable, accounts receivable, taxation, payroll and the preparation of Treasury, financial and management reports.

The Finance unit keeps records relating to tenants and includes name, address and trading figures. This unit also sources goods and services.

5.1.2 External Relations

This unit provides corporate stakeholder management, ministerial liaison, media monitoring, and maintains a list of Ministerial contacts. The corporate secretarial function resides within this unit as does Legal Services and the Design Studio.

The Design Studio includes graphic design and production of the Authority's corporate, sales and marketing materials. Supplier details are held eg printers and software support company contact information.

5.1.3 Human Resources

The Human Resources unit deals with staff recruitment, payroll, learning and development, organisational development, dispute resolution and termination / resignation. The unit also manages the e-learning program on privacy.

The Human Resources unit holds individual files on all employees involving personal information. This includes information such as name and address, date of birth, next of kin, rate of pay, leave claims, increments, and Equal Employment Opportunity (EEO) information.

Also included may be matters of a disciplinary or development nature. This unit also collects health information by way of medical certificates for sick leave and injury report forms.

5.1.4 Information, Communication and Technology (ICT)

The ICT unit provides information technology services to the Authority. It maintains the Local Area Network (LAN) as well as computer hardware and software.

The E-services team develop web services including databases on the intranet. The ICT unit also encompasses the Authority's records management function.

5.1.5 Procurement

This section drafts tenders, quotations and contracts for the Authority, oversees tender documentation, and retains information electronically, relating to the Authority's suppliers and contracts.

5.2 MARKETING AND EVENTS

The units within Marketing and Events are:

- Educational Services
- Marketing
- Events
- Sydney Visitors Centre
- Business Development and Venue Hire

5.2.1 Educational Services and Tours

The information held by this unit includes contact details for casual staff and emergency contact details for full time staff, emergency contact mobile phone numbers for teachers accompanying students on booked programs, a database of contacts and information gathered through Sydney Learning Adventures bookings, marketing and tourism promotion initiatives, and a database of NSW and ACT schools (from Department of Education and Training).

5.2.2 Sydney Visitors Centres

The Sydney Visitor Centre The Rocks and Darling Harbour (SVC) keeps contact details for all SVC staff. The SVC also acts as an agent for tour operators, hotels and service providers and maintains a database of contact details for these client businesses. Similarly, the SVC maintains records of retail product suppliers for business purposes.

Financial data records are also maintained for travel booking and retail purchase transactions generated through the SVC.

Limited salaries data is kept by the SVC managers for the purposes of responding to employee's pay enquiries.

5.2.3 Marketing

Rocks Experience database, Rocks Experience subscribers can unsubscribe online, or can contact the Authority by phone, fax or email and their details will be moved from that database and placed in the 'removed' database and kept on file for one year before being deleted off the database. Rocks Event and Experience Magazine competitions along with Club Darling Harbour and Rewards@TheRocks information is kept until the competition is drawn and used to contact the winner. This information is then filed.

Photobooth subscribers, this data is not currently used, however once new email marketing software is implemented, communication will also be sent to these members.

Subscribers can opt-out at any time by contacting the Authority by phone, fax or email.

5.2.4 Business Development and Venue Hire

Functions include sponsorship procurement, cooperative marketing, banner program sales and venue hire. Information held by this department includes client database (held in the Event Business Management System), Authority casual staff contact details, contracts and other general information relating specifically to the Authority's core business.

5.3 STRATEGIC DEVELOPMENTS

The Strategic Developments division is involved in managing land sales, facilitating the development of sites and assets and preparing master plans and development applications. Information of a confidential nature is contained in tender documents which may ask for proof of financial standing of individuals or company directors.

5.4 PROPERTY AND ASSET MANAGEMENT

This division is responsible for urban design and planning, including heritage and archaeology, capital works operations and maintenance of services and facilities. This division also provides property services to the Authority's tenants. Additionally, the division processes applications under the *Heritage Act 1977* for works on properties listed in the

Heritage Register, and manages insurance claims. See **Section 7.1.7, Implementing the Privacy Management Plan, Complaints and Insurance Claims**. Personal information held by the division includes contractor details and limited staff information.

5.4.1 Property Management

This unit acts as landlord to the Authority's tenants and ensures the continued viability of the Authority's precincts. It also operates The Rocks Markets.

The division collects and holds information on all tenants and licence holders (market stalls) and lease documents. This information includes name and address of residential tenants as well as financial and trading history of retail and commercial tenants.

5.4.2 Assets and Facilities Management

The Asset Services Group is customer focused in meeting the needs of internal and external stakeholders, providing comprehensive portfolio support services including facilities management and asset planning, capital works and special projects delivery, heritage, design and sustainability advice, operations management including security, ranger services, compliance, horticulture, cleaning and waste, and program administration incorporating budget management, requisitions and the customer request management system (CRMS).

6 EXISTING POLICIES AND LAWS RELATING TO INFORMATION

The Authority is aware of concerns of privacy and confidentiality and exercises discretion in its actions. The Authority has issued a *Code of Conduct for Staff Members*, which gives staff clear guidelines to the use, or misuse, of information. The Authority conducts regular staff training sessions in relation to the Code.

7 IMPLEMENTING THE PRIVACY MANAGEMENT PLAN

7.1 CLASSES OF PERSONAL INFORMATION

The Personal Information classes include:

- Personnel/staff records
- Administrative records
- Tenant records
- Contractor/supplier records
- Security and Ranger records
- Development Applications
- Complaints and Insurance Claims
- Mailing Lists
- Corporate Database.

The classes are detailed as follows:

7.1.1 Personnel/staff records

Official personnel files are held in a secure environment in the Human Resources section. The records include details such as addresses, date of birth, next of kin, nature of employment, salary and bank account details. Also included may be position applications and resumes, notes of a disciplinary/developmental nature and EEO data.

State Records Guidelines are observed in relation to the retention and disposal of HR Records for staff that have left the employment of the Authority. The resumes of unsuccessful applicants are disposed of in security bins.

The Authority is aware pursuant to s.(3)(i) of the *Privacy and Personal Information Act 1998*, that information or an opinion about an individual's suitability for appointment or employment as a public sector official is not personal information for the purposes of the Act.

7.1.2 Administrative records

Administrative records include contact details for Board members, as well as Freedom of Information requests.

7.1.3 Tenant records

Records are kept on tenants' financial history including current and past trading and rental payments. Files also record lessees' contact details, bank account number and the usual documents associated with commercial leases.

7.1.4 Contractor / supplier records

Contractors, and in some cases consultants, are asked to provide proof of financial standing when being considered for a tender. Information includes financial records as well as company structures and curriculum vitae of tenderer's staff.

7.1.5 Security and Ranger records

The Foreshore Authority employs a Security and Logistics Manager who manages security and ranger services for the Authority's major tourist precincts. The Rangers and the Security and Logistics Manager collect the following information:

- **Daily Occurrence logs.** These logs record general patrols, observations and minor incidents.
- **Security Officer log books.** Log books are for security officers' notes during patrols and investigations. Incidents and occurrences are recorded which might include names and addresses.
- **Incident Reports.** Incidents or complaints of more than a minor nature are recorded on an incident report. Information might include names and addresses of complainant, offenders, victims and witnesses of offences.
- **Injury Reports.** Rangers may compile reports on injuries sustained by visitors.
- **Security monitoring.** Businesses with back to base alarms have their systems monitored through a contract-monitoring centre. Logs can identify individuals and times of activity.
- **Internal security.** The Security and Logistics Manager issues staff security passes and keeps a log of after hours access. The passes are collected on resignation from the Authority.
- **Closed circuit surveillance cameras** are operated within the Authority's precincts. The tapes are randomly viewed in the event of any major incident. Police may request footage of specific incidences, but this will only be provided if a formal request is authorised by the Police. Surveillance footage will only be provided to persons other than the Police, on the production of a subpoena.
- **Parking Permits** are issued to approved Authority staff and contractors where required.

7.1.6 Development Applications

Since December 2008, the Authority no longer has planning delegations. However the Authority is required, under the *Environmental Planning and Assessment Act 1979*, to maintain a register of development applications processed prior to that date for public inspection, together with records of development permits containing the conditions that must be satisfied in relation to particular developments. The register contains minimal personal information.

7.1.7 Complaints and Insurance Claims

The Authority has systems to receive and deal with individuals' complaints and insurance claims.

7.1.8 Mailing Lists

Various mailing lists are maintained throughout the Authority which include contact details of stakeholders, tourist and marketing organisations, suppliers, consultants, contractors and individuals who have requested to be put on a mailing list to receive information concerning events and special promotions. Forms seeking names and addresses for making lists include a Privacy Statement.

7.1.9 Corporate Contacts Database

The Authority has developed a corporate contacts database that various sections are able to access. However, each section is only able to access that part of the database that relates to that section. Staff accessing and/or updating the database have been made aware of their responsibilities.

7.2 HEALTH INFORMATION

This section addresses the seven main headings of the Health Privacy Principles which are:

- Collection
- Storage
- Access and Accuracy
- Use
- Disclosure
- Identifiers and Anonymity
- Transferrals and Linkage

7.2.1 "Collection"

Health information is collected by way of medical certificates in support of sick leave and advice from a medical practitioner if an injury is work related. The certificates are provided by the staff member, unless sent direct by a medical practitioner in cases of prolonged absence of staff from work for medical reasons.

7.2.2 "Storage", "Access and Accuracy", "Use", "Disclosure"

The certificates are retained on file in a secure environment and only used for the purposes collected.

7.2.3 "Identifiers and Anonymity", "Transferrals and Linkage"

No medical identification numbers are issued by the Authority. When completing an Injury Report Form staff are advised that any information relating to the injury may be transferred to the Authority's insurers.

8 COMPLIANCE WITH THE PRIVACY IPPS

8.1 COLLECTION OF INFORMATION

IPPs 1,2,3,4 apply

The Authority collects information as detailed in **Section 7.1, Implementing the Privacy Management Plan, Classes of Personal Information.**

Information is only collected which is directly related to the activities and functions of the Authority.

Personal information is collected directly from the individual unless the individual has authorised someone else to provide information on their behalf. An exception to this is staffing information which is retained on files maintained securely in the Human Resources section. However, staff can review their own information at any time.

The Authority informs individuals that information is being collected, the purpose of collecting the information and the intended recipients. A privacy provision is included on forms and an audit has been undertaken to ensure that forms address privacy provisions.

8.2 STORAGE

IPP 5

Information is stored both electronically and on paper. The Authority's compliance or otherwise is detailed as follows:

8.3 STORING INFORMATION - CORPORATE SERVICES

8.3.1 Corporate Secretary

Paper files relating to FOI requests, responses and information relating to the Board are kept in a lockable cabinet in the Corporate Governance work area. Electronic files are stored on the network and are secured by password.

8.3.2 Finance

Files relating to debtors' payments are stored electronically. Electronic files are stored on the network and are secured by password.

8.3.3 Human Resources

All paper files are kept in a secure storeroom environment. Electronic files are stored on the network and are password protected. Staff can inspect their paper file at any time.

8.3.4 Information, Communication and Technology

The Manager, ICT, has access to all files on the network through the administrator's password access. Staff in this section have access to the Authority's records system. The State Records Guidelines are observed in relation to the retention and disposal of Human Resources and other records.

8.3.5 E-Services

All data is stored electronically. Data is stored in secure databases with limited access.

8.4 STORING INFORMATION – MARKETING AND EVENTS

Contact details are kept in lockable files or held on the personal files of key staff. Electronic files are password protected.

8.4.1 Sydney Visitor Centres

Files relating to client businesses are stored in lockable cabinets within a secure office. Electronic files are password protected. Salaries information is stored in the same manner.

8.5 STORING INFORMATION – STRATEGIC DEVELOPMENTS

This unit stores all material of a confidential nature in a secure storeroom. Electronic files are stored on the network and are password protected.

8.6 STORING INFORMATION – PROPERTY AND ASSET MANAGEMENT

Paper files are stored in lockable cabinets. Electronic files are stored on the network and are password protected. This unit also has a secure storeroom. Access to closed circuit surveillance material by the Police or staff request must be authorised by the Security and Logistics Manager.

8.6.1 Property Management

Paper files and leases are stored in lockable cabinets or in locked file rooms. Electronic files are stored on the network and are password protected.

8.6.2 Assets and Facilities Management

Paper files are stored in lockable filing cabinets. Access to electronic documents is limited. Information regarding personal and company details, motor vehicle registration details are recorded in on-line systems requiring password access.

8.7 NOTIFICATION, ACCESS AND CORRECTION

IPPs 6 – 10

IPP – 6. The Authority includes a privacy provision on forms when personal information is being sought. The provision includes the reason for collection, storage, the purposes of the information and details of any third party involvement.

IPP – 7. Staff can review information on their personnel file for accuracy. Any amendment to file records must be made by the Human Resources Manager to ensure such changes meet with the guidelines of the Privacy Management Plan.

IPP – 8. This principle commits the Authority to allowing personal information to be corrected in order to ensure accuracy. The Authority is committed to ensuring that all information it holds is accurate and complies with this principle.

IPP – 9. This principle obliges the Authority to try to ensure that all personal information that it collects or holds is relevant. Mailing lists and other records are updated from time to time to ensure currency and staffing information is archived when a staff member leaves the employment of the Authority.

IPP – 10. The Authority does not use personal information for any purpose other than for which it was collected. This principle has been reinforced through staff training.

8.8 DISCLOSURE

IPP – 11

In accordance with principle 11 (Section 18), personal information is not disclosed to third parties except where disclosure is directly related to the purpose for which the information was collected.

In such instances, the individuals concerned would be aware that disclosure of personal information is either necessary to perform a service or carry out a function, or the Authority is satisfied that the disclosure is not contentious to the individual concerned. This includes:

- Contact details that are referred to mailing houses to distribute information to individuals who have requested information about the Authority.
- Contact details and incident reports that are forwarded to the Authority's insurer to access an insurance claim.
- HR files owned by the Authority.
- Legal requests, such as subpoenas.

An exemption from compliance with principle 11 is:

Where disclosure is required under legislation in accordance with the exemption provided under section 25 of the *Privacy Act* "*Exemptions where non compliance is lawfully authorised or required*". Specifically, the *Environmental Planning and Assessment Act 1979* requires the Development Applications Register to be open to public inspection.

IPP – 12

The Authority does not disclose information relating to an individual's ethnic or racial origin, and other related sensitive personal information except where:

Exemption from compliance is provided under section 23(7) of the *Privacy Act* "*Exemptions relating to law enforcement and related matters*".

Personal information relating to an individual's alleged racial or ethnic origin may be reported to the Police where:

"disclosure of the information is reasonably necessary in order to investigate an offence where there are reasonable grounds to believe an offence has been committed or may be committed."

Ethnic and racial information is also part of the Workforce Profile. Whilst names are not used, some statistics could provide sufficient details for individuals' identity to be linked to the statistics. Principle 12 also places restrictions on disclosure of personal information to jurisdictions outside NSW, however, there is generally no reason why personal information is provided to other States or internationally.

8.9 PROTECTION OF PERSONAL INFORMATION

Human Resources Department gathers and holds personal identifying information and has a requirement to send it by post. This occurs when it sends a Tax File Number Declaration to the Taxation Office or a Group Tax Summary to an employee.

To ensure suitable protection of personal information, the Authority sends such information via 'Express Post' to allow the item to be tracked and delivery confirmed if necessary.

8.10 COMPLIANCE WITH THE PUBLIC REGISTER PROVISIONS

The Authority is aware of the provisions relating to information kept on Public Registers in the Act. In general the amount of personal information it collects is limited. The personal information that might appear on a Public Register (such as lists of Development Applications) would be little more than name and address.

9 THE INTERNAL REVIEW PROCESS

This section examines the Internal Review Process of how the Authority handles complaints from any individual (public or employee) about the use of their personal information. Under Part 5 of the Act there are clear procedures to be followed in response to any complaint. An Application for Internal Review is appended to this document (Appendix 3).

9.1 WHO CAN CALL FOR A REVIEW?

Any individual (the applicant) who believes that they have a case for grievance against the Authority is entitled to call for a review of the Authority's conduct (this is not necessarily limited to conduct which directly affects the applicant). The person calling for an internal review must write to the Authority within 6 months (or longer as agreed by the Authority) of becoming aware of the breach of privacy. The letter must contain the sender's address in Australia and should ideally include contact phone numbers.

9.2 WHAT ACTIONS MIGHT PRECIPITATE A REVIEW?

An individual is legally entitled to call for an internal review when they believe the Authority has broken an Information Protection Principle (IPP); broken a privacy code of practice; or has disclosed personal information from a public register.

9.3 WHO DEALS WITH INTERNAL REVIEWS?

Internal reviews will normally be conducted by the Legal Services Manager, or another employee as may be nominated by the CEO. The employee appointed will not be substantially involved in the matter of complaint; and will be suitably qualified to deal with the matters raised.

9.4 WHAT THE AUTHORITY MUST DO

- Complete the review as soon as practical. If the review is not completed within 60 days from the day on which the application is received, the applicant can make an application under Section 55 to the Tribunal for a review of the conduct concerned.
- Consider all relevant material submitted by the applicant and the Privacy Commissioner.
- Notify the Privacy Commissioner as soon as practical that a review is underway.
- Within 14 days after the completion of the review notify the applicant of the findings of the review (and the reasons for the findings); the action that the Authority is proposing; the right of the applicant to have the Authority's proposed actions reviewed by the Tribunal.
- Keep the Privacy Commissioner informed of progress of the review.
- Inform the Privacy Commissioner of the findings of the review and of the proposed action.

9.5 HOW THE AUTHORITY RESPONDS TO A REVIEW

Following the completion of the review the Authority may:

- take no further action on the matter
- make a formal apology

- take such remedial action as it thinks appropriate (ie: the payment of monetary compensation)
- provide undertakings that the conduct will not occur again
- implement administrative procedures to ensure that the conduct will not be repeated.

9.6 WHAT HAPPENS IF A PERSON IS NOT SATISFIED WITH AN INTERNAL REVIEW?

If the applicant is not satisfied with the findings of the review, or with the action taken by the Authority in relation to the findings, they can apply to the Tribunal for a review of the Authority's conduct in this matter. The Tribunal has a number of actions available to it as noted in the Act [54, (2)]. These actions include the power to order payment of up to \$40,000 in compensation.

10 DISSEMINATION OF POLICIES AND PRACTICES

Dissemination of the policies and practices of the Act is vital to the implementation of the Plan. The Authority aims to make its Privacy Management Plan (the Plan) available both internally and externally. Enquiries are to be directed to: The Manager, Corporate Governance, Sydney Harbour Foreshore Authority.

Staff are required to complete an e-learning module on privacy to ensure that they have a knowledge of the principles involved. The Authority has developed an intranet site for the information of staff and the Privacy Management Plan is made available on the site. It is the intention of the Authority to have the Plan published on its Internet site which is available to anyone with Internet access. Copies of the Plan will be made available free of charge to any member of the public who requests it.

11 CODES OF PRACTICE

The Authority is bound by the "Privacy Code of Practice for the NSW Public Sector, Workforce Profile" issued by the NSW Premier's Department in 1999.

The classes of information this Code applies to include:

- Biographical, including EEO data provided by employees for the purpose of developing and monitoring equal employment opportunity management plans
- Employment status (ie: permanent, temporary, casual, etc.)
- Remuneration levels (totals and some specific payments such as overtime and higher duties allowance)
- Leave accruals and leave taken (recreation, sick etc.)
- Movement in and out of the sector (recruitment of separation).

12 DISCLOSURE OF PERSONAL INFORMATION OUTSIDE NSW

Disclosures made outside NSW are not affected by the Act. However, all IPPs, and specifically Section 19 (2) of the Act, will be observed by the Authority when responding to any requests for personal information from outside NSW.

Management Plan

Key performance indicator : compliances with the Information Protection Principles (IPPs)

Objectives	Strategy	Responsibility	Time Frame
1. Ensure that staff records contain only information that is accurate, up to date and complete – in compliance with IPP4.	Permit staff to have access to their personal information held by the Authority.	Human Resources Manager	On-going
2. Ensure that individuals are aware of their rights and obligations in relation to the collection, use and storage of personal information.	Encourage all existing and new staff to read and become familiar with the Authority's Privacy Management Plan. Provide free and easy access to the Privacy Management Plan – Intranet. Review all data collection forms to ensure that each form clearly states the purpose for which data is being collected.	Corporate Secretary Corporate Secretary Corporate Secretary	On-going On-going Ongoing
3. Ensure that all staff, consultants and contractors are aware of the Privacy Management Plan and are able to practice the IPPS.	New staff to be made aware of the Plan as part of their induction. Existing staff to be reminded of the need to be vigilant in the protection of individual's privacy.	Human Resources/Corporate Secretary Corporate Secretary	On-going On-going
4. Ensure the timely and secure disposal of records.	Ensure disposal of records in accordance with records disposal policy. Be aware of and follow the principles in the State Records Act 1998.	Records Co-ordinator Records Co-ordinator	Ongoing Ongoing

13 CONTACTS/REFERENCES

13.1 CONTACTS

The Corporate Secretary is the Foreshore Authority's Privacy Officer and should be contacted on privacy matters.

13.2 RELEVANT LEGISLATION

- Privacy and Personal Information Protection Act 1998
- Health Records and Information Privacy Act 2002
- Freedom of Information Act 1989
- Heritage Act 1977
- Environmental Planning and Assessment Act 1979

13.3 OTHER RELEVANT POLICIES/PUBLICATIONS

- Privacy NSW's Guide to Making Privacy Management Plans.

14 APPENDICES

This information can be found in the following Appendices:

- **Appendix A** – Definitions
- **Appendix B** – Information Protection Principles in Application
- **Appendix C** – Application for Review of Conduct
- **Appendix D** – Review of Conduct – Authority Checklist

14.1 APPENDIX A – DEFINITIONS

Confidentiality: An obligation which restricts an agency from using or disclosing any information which is contrary to the interests of the person or organisation which provided it in the first place. This information need not be personal information for confidentiality to apply. In addition, confidentiality often exists because of legal or ethical professional obligations (e.g. like those of doctors and lawyers). Confidentiality often arises from the circumstances in which information is given to someone, for example, from relationships of trust and reliance.

Information Protection Principles: Principles in the *Privacy and Personal Information Protection Act 1998* protect the privacy rights of individuals in relation to the collection, storage, use and disclosure of personal information by NSW public sector agencies.

Personal Information: Information or opinion about an individual whose identity is apparent or can reasonably be ascertained from the information or opinion.

Privacy: Applies to personal information irrespective of who provided it to the agency. Bearing this in mind, the Information Protection Principles (see definition) pay as much attention to matters such as collection and storage as they do to use and disclosure. Privacy principles exist in addition to any obligations of confidentiality.

Public Register: A register of personal information that is required by law to be, or is made, publicly available or open to public inspection.

The Tribunal: The Administrative Decisions Tribunal.

Appendix B – Information Protection Principles in Application

A summary of the principles in the *Privacy and Personal Information Protection Act 1998* as applied to function, is listed below:

14.1.1 Collection of Personal Information

1. Collection of personal information must be for a lawful purpose that is directly related to a function or activity of the Authority and must be reasonably necessary.

(Section 8)

2. Personal information must be collected by lawful means and must generally be collected directly from the individual to whom the information relates

(Section 9)

3. The Authority must make the individual aware of the following:

- the fact that the information is being collected
- the purpose for which the information is being collected
- the intended recipients of the information
- whether the supply of information by the individual is required by law or is voluntary and any consequences for the individual if the information is not provided
- the existence of any right of access to, and correction of, the information.

(Section 10)

4. The Authority must take reasonable steps to ensure that the information collected is relevant to the purpose, is not excessive, is accurate, up to date and complete.

(Section 11)

14.1.2 Use/Disclosure of Personal Information

5. Personal information must be protected against loss, unauthorised access, use, modification or disclosure and against all other misuse.

(Section 12)

6. If it is necessary for personal information to be given to a person in connection with the provision of service of an agency, everything reasonably within the power of the Authority is done to prevent unauthorised use or disclosure of the information

7. The Authority must check the accuracy of personal information before use.

(Section 16)

8. The Authority must not use personal information for a purpose other than that for which it was collected unless:

- the individual to whom the information relates has consented to the use of the information for that other purpose; or
- the other purpose for which the information is used is directly related to the purpose for which the information is collected; or
- the use of the information for that other purpose is necessary to prevent or lessen a serious and imminent threat to the life or health of the individual to whom the information relates or of another person.

(Section 17)

9. The Authority must not disclose personal information unless:
- the disclosure is directly related to the purpose for which the information was collected and there would be no reason to believe that the person would object to such disclosure;
 - the individual concerned is reasonably likely to have been aware, or has been made aware, that information of that kind is usually disclosed to that other person or agency;
 - the Authority believes on reasonable grounds that the disclosure is necessary to prevent or lessen a serious and imminent threat to the life or health of the individual concerned or another person.

(Section 18)

10. The Authority when provided with personal information from another agency must not use or disclose the information for a purpose other than the purpose for which the information was given to it.

(Section 18)

11. The Authority must not disclose personal information relating to an individual's ethnic or racial origin, political opinions, marital status, religious or philosophical beliefs, trade union membership, health or sexual activities unless the disclosure is necessary to prevent a serious or imminent threat to the life or health of the individual concerned or another person.

(Section 19)

12. The Authority must not disclose personal information of an individual to any person or body who is in a jurisdiction outside NSW unless:
- a relevant privacy law that applies to the personal information is in force in that jurisdiction (to be determined by the NSW Privacy Commissioner), or
 - the disclosure is permitted under a code of practice (to be determined by the NSW Privacy Commissioner).

NB: This principle will apply when the Code of Practice is established.

(Section 19)

14.1.3 Access/Amendment of Personal Information

13. The Authority must take all reasonable steps to enable a person to ascertain whether the agency holds personal information relating to that person and if so, the nature of that information; the main purpose for which the information is used; and that person's entitlement to gain access to the information.

(Sections 13 and 14)

14. Individuals have a right to have personal information about them amended to ensure that the information is accurate, relevant, up to date, complete and not misleading.

(Section 15)

14.1.4 Retention Personal Information

15. Personal information must only be maintained for as long as is necessary for the purposes for which the information may be lawfully used.

(Section 12)

14.1.5 Disposal Personal Information

16. Personal information must be disposed of securely.

(Section 12)

14.2 APPENDIX C – APPLICATION FOR REVIEW OF CONDUCT

Application for review of conduct under section 53 of the Privacy and Personal Information Protection Act 1998

1. Your full name

2. Your residential address

3. Your postal address (if different from your residential address)

4. What is your complaint?

5. When did the conduct you are complaining about occur? (be as specific as possible)

6. When did you become aware of the conduct?

7. What effect did the conduct have on you or another person?

8. What effect could the conduct have on you or another person?

9. What would you like to see the Authority do about the conduct?

I understand that details of my application will be referred to the Privacy Commissioner in accordance with section 54(1) of the *Privacy and Personal Information Protection Act 1998* and that the Privacy Commissioner will be kept advised of the progress of the review.

Signature of Applicant

Dated:

14.3 APPENDIX D – REVIEW OF CONDUCT – AUTHORITY CHECKLIST

Application for review of conduct under section 53 of the Privacy and Personal Information Protection Act 1998

Page 2 AUTHORITY CHECKLIST (Authority use)

10. Is the complaint a matter which involves a possible breach of the Privacy and Personal Information Protection Act or a code made under the Act?

Yes – go to question 11

No – follow the Authority’s normal complaint handling procedure

11. When was the request for review first received?

12. When will the 60 day period for completion of the review elapse?

13. Was the Privacy Commissioner notified of receipt of the request and been invited to make submissions?

14. Has the Privacy Commissioner been asked to conduct the review on behalf of the agency?

15. Has the applicant provided the necessary information under section 53(3) of the Privacy and Personal Information Protection Act?

16. Nominate the IPP, code section or public register provision to which the conduct relates.

17. Is the request being dealt with by an officer who was not substantially involved in the subject matter of the request for review?

18. Name, designation and contact number of person now dealing with the complaint.

19. Preliminary comments by the agency and/or the Privacy Commissioner in relation to the application.

20. What was the outcome of the review?

21. Was the applicant notified of the outcome of the review, the proposed action and their right to seek a review of the findings within 14 days of the review being completed?

Signature of Authorised Officer _____