Privacy Management Plan

27 November 2023

Issued for: Landcom

Issue date: 27 November 2023

Distribution only: External

Issued and authorised by: Chief Executive Officer

Version: 1.0

LANDCOM

Creating more affordable and sustainable communities

Contents

1 Privacy Management Plan overview

1.1 Why Landcom has a Privacy Management Plan

This Privacy Management Plan (PMP) explains how Landcom manages personal and health information in line with NSW privacy laws, namely:

- The *Privacy and Personal Information Protection Act 1998 (NSW)* (PPIP Act) which protects 'personal information', and
- The *Health Records and Information Privacy Act 2002 (NSW)* (HRIP Act) which protects 'health information'.

Section 33 of the PPIP Act requires certain NSW government agencies like Landcom to have a PMP. Landcom's PMP sets out our commitment to protect privacy for our purchasers and members of the public, applicants for positions, current and former Staff, contingent workers, people working for our suppliers, and other stakeholders.

Landcom has always been legally bound by the HRIP Act, but the PPIP Act did not apply to state-owned corporations like Landcom until it was amended in 2022. Although Landcom has voluntarily elected to comply with the PPIP Act in the past, from 28 November 2023 when the amendments to the PPIP Act commence, Landcom will be legally regulated under the PPIP Act.

Our PMP explains:

- How we develop policies and practices to ensure compliance with NSW privacy laws, and how we train our staff on their use;
- Who you can contact if you have any questions about the personal and health information we collect and hold;
- How you can access or amend your personal and health information;
- What you can do if you have concerns about privacy protection, or the way Landcom manages personal and health information; and
- Other matters we consider relevant to the PMP in relation to privacy and the personal and health information we hold.

Several terms and abbreviations are used in this PMP. Some of them are also used in the NSW privacy laws. These terms and abbreviations are listed in the Glossary in section 8.

1.2 How we promote our Privacy Management Plan

Landcom will use this PMP to train our Staff to handle personal and health information responsibly, transparently, respectfully, and securely in accordance with the PPIP Act and HRIP Act. We will also use and update the PMP when we implement new projects or systems that may change the way we manage personal and health information.

We will promote our PMP through:

- Our Executive Committee (ExCo) – by having ExCo members endorse the PMP and any significant variations made over time;
- Our Staff:

  - We will include the PMP as a resource in online training for new Staff, and in targeted privacy training for Staff in Landcom divisions where personal information handling is a dominant activity;
  - We will ensure that Staff consider the impact of PMP commitments on, and alignment with, any activities involving management of personal and health information;
  - Our Staff can access and use the PMP (in addition to consulting their manager or our Privacy Officer) as an initial step if they have any questions about management of personal or health information;
  - We will give our contingent workers access to the PMP. We will also train them on their privacy obligations if necessary for their role; and
  - We will ensure our Board is given a copy of the PMP and made aware of Landcom's privacy requirements and any relevant areas of risk.
- Public awareness measures, including:
  - We will publish the PMP on Landcom's website, www.landcom.com.au. We can also make it available via mail or collection upon request;
  - We will reference the PMP in privacy collection statements and/or consent forms issued to people when collecting personal information from them directly;
  - By having the PMP translated into other languages or accessible formats if requested or required; and
  - By informing people about the PMP where it may assist in answering questions about how Landcom manages personal and health information.

Our PMP is an integral part of Landcom's corporate governance, intended to assist in guiding not only our operations but our ongoing compliance monitoring and business improvements.

Our PMP is also intended to align with current guidance on PMPs issued by the NSW Information and Privacy Commission (IPC), the NSW Government agency who regulates both the PPIP Act and the HRIP Act.

2 About Landcom

2.1 Context and objectives

Landcom is a state-owned corporation established under the *State Owned Corporations Act 1989* (NSW) and the *Landcom Corporation Act 2001* (NSW).

Our principal objectives are found in Section 6 of the *Landcom Corporation Act 2001 (NSW)*.

Landcom is a NSW Government owned development organisation. We are a commercial business that develops land to achieve both public outcomes and financial benefits for the NSW Government and the people of NSW. We do this by:

- Supplying home sites through the delivery of sustainable master planned communities and development projects, with a focus on expanding the stock of affordable and diverse housing; and

- Enabling development by de-risking and unlocking strategic and complex sites in collaboration with landowners and the market.

To help the NSW Government deliver its urban management objectives we are focussed on four goals:

- Increasing housing supply;
- Leadership in Affordable Housing;
- Expansion into regional NSW; and
- Build to Rent pilot program in regional NSW.

Our firm commitment to leadership in sustainability and climate resilience applies to each of these goals.

More information about Landcom's functions, governance, projects and activities can be found on the Landcom's website (at www.Landcom.com.au).

3 Landcom strategies for compliance and best practice

Landcom adopts several strategies to implement best practice principles and comply with our obligations under the PPIP Act and the HRIP Act. These strategies recognise that privacy is a shared responsibility within Landcom.

3.1 Privacy laws

Landcom's privacy-related obligations are in two NSW privacy laws:

- the *Privacy and Personal information Protection Act 1998 (NSW)* (PPIP Act); and
- the *Health Records and Information Protection Act 2002 (NSW)* (HRIP Act).

The PPIP Act protects 'personal information' which includes things like an individual's name and address, family life, ethnic background, financial information, or a photo or video that readily identifies them.

Health information is a more specific type of personal information. It can include information about a person's physical or mental health (e.g. a disability, disability needs and supports, or a mental health report). Although we do not provide health services and do not manage a lot of health information, any health information we do collect must be managed in line with the HRIP Act.

The PPIP Act also governs how NSW government agencies should manage personal information contained in public registers. Landcom doesn't maintain any public registers, so these requirements do not apply to us.

There are other laws which require personal or health information to be handled in a particular way – such as income tax and workplace safety laws, and the *Public Interest Disclosures Act 2022 (NSW)*. These laws affect our information handling in the same way they impact any other NSW government agency.

3.2 Landcom policies relating to or supporting privacy management

Landcom has official policies relating to many of our activities to help ensure compliance with the requirements of privacy legislation and support privacy management by following a rigorous policy review and approval process. Some of these policies and publications are available on Landcom's website (Landcom Policies - Landcom).

Landcom's Privacy Framework is a suite of resources for Landcom staff including this PMP, template collection notices, factsheets, checklists and links to the PPIP Act and HRIP Act. Key privacy-related policies and documents include our:

- Privacy Statement, on the Landcom website;
- Data Breach Policy;
- Moderation Policy and Etiquette Guide – for management of online discussion forums (a webpage);
- Join-in – Engagement Charter;
- Social Media Terms of Use (Webpage);
- Complaints Handling Policy;
- Records Governance Policy and Procedure;
- Customer Relationship Management (CRM) Data Retention & Disposal Procedure;
- ICT Information Security Policy;
- Staff Code of Conduct;
- Supplier Code of Conduct;
- Fraud Control and Corruption Prevention Policy;
- Handling Conflicts of Interest Policy;
- Public Interest Disclosure Policy;
- Data Breach Notification Procedure; and
- Workplace Surveillance Procedure.

We also consider other NSW government policies and frameworks which support privacy management over a range of functions, such as the procurement of ICT services and cyber security.

3.3 Privacy awareness

Landcom undertakes a range of initiatives to ensure its Staff, Suppliers and members of the public are informed of our privacy practices and obligations under the PPIP and HRIP Acts.

This includes promoting privacy awareness and compliance by:

- Publishing and promoting this PMP on our intranet and website;
- Publishing a Privacy Statement on the Landcom website, Landcom.nsw.gov.au;
- Publishing and promoting a dedicated Privacy Framework page on our intranet, which centralises all privacy resources for Staff and provides clear information about what to do if Staff are unsure about privacy issues;

- Publishing privacy factsheets on our intranet or providing links to IPC factsheets to provide Staff with practical guidance on privacy issues and considerations;
- Including a privacy module in our onboarding program for all new Staff; and
- Delivering periodic face to face or online targeted training across different business areas as required.

3.4 Roles and responsibilities

3.4.1 Our Staff and Suppliers

All Landcom Staff are required to comply with the NSW privacy laws. Both the PPIP Act and HRIP Act contain criminal offences that would apply to Staff, former Staff, and the people we engage. For example, it is an offence to:

- Intentionally use or disclose personal or health information for an unauthorised purpose;
- Offer to supply personal or health information for an unauthorised purpose; or
- Hinder a member of the IPC's staff from doing their job.

Suspected criminal conduct may result in dismissal and/or reporting to other agencies for criminal investigation. This includes offences under NSW privacy laws, information about which is available on the IPC website. In addition, Staff suspected of conduct that would breach the NSW Privacy Principles or the offence provisions in relevant privacy laws may also breach the Staff Code of Conduct or other applicable Landcom policies.

Similarly, our Suppliers are subject to a Supplier Code of Conduct which outlines Supplier confidentiality obligations. Our agreements with Suppliers contain specific requirements aimed at protecting personal and health information. In particular, information must only be used for the purposes for which it is given, and its confidentiality must be maintained.

3.4.2 Landcom's Privacy Officer

The Privacy Officer in Landcom's Legal team is responsible for:

- Collaborating with Landcom's Executive Committee and relevant Divisions to develop our PMP;
- Developing, disseminating, and embedding the PMP through staff awareness and training;
- Developing, reviewing and maintaining other Landcom privacy-related policies;
- Privacy reporting obligations, including for Landcom's annual reports;
- Consulting with the IPC on any high privacy risk programs or incidents;
- Ensuring relevant privacy related policies and procedures are regularly reviewed and made available through Landcom's website and/or intranet;
- Assisting with advice and direction on the processing of requests for personal or health information under the PPIP Act, HRIP Act or the *Government Information (Public Access) Act 2009* (NSW) (GIPA Act); and
- Coordinating and, where appropriate, investigating any privacy breaches or complaints.

You can contact our Privacy Officer for further information about this PMP, and:

- The personal and health information we hold, and how we manage it;

- To request access to or amendment of personal or health information;
- To request an internal review about a breach of the PPIP Act or HRIP Act; or
- For any other privacy-related concerns.

Contact details: Privacy Officer, Landcom
Address: PO Box 237 PARRAMATTA NSW 2124
Phone: (02) 9841 8626
Email: privacy@landcom.nsw.gov.au

4 Key functions that involve management of personal information

4.1 Our public engagement work

As the NSW Government's land and property development organisation, our activities include master planning and partnering with the private sector to deliver strategic and complex development projects on vacant or established sites. We also focus on delivering the local infrastructure that new communities need to grow and thrive. Our operations span across Greater Sydney and are expanding into regional NSW.

To succeed in this work, we need meaningful participation of the many people and groups who have a stake in the evolution of our cities and the new places that we are tasked to deliver. This includes seeking participation from the public and the local communities who know these places best.

Landcom is committed to excellence in stakeholder engagement and has an overarching engagement framework called 'Join In', which provides a charter and protocol to guide our engagement practice. We prepare and implement stakeholder engagement and communication strategies for all projects. Information about projects is on our website: www.landcom.com.au and project-specific websites accessed from the main webpage.

In terms of personal information, much of our engagement work involves collecting only basic contact details from our stakeholders. We enable interested stakeholders to sign up (and unsubscribe at any point) for updates on our projects and activities via the Landcom website. We engage stakeholders throughout the planning process on each project and deliver community development programs for a number of our projects, which help establish a sense of place and community cohesion as places grow and change.

We use a range of engagement approaches to suit different communities and reflect the specific purpose of our engagement. These may include, for example, community information sessions, online consultation, workshops, surveys and focus groups. We use our website, www.landcom.com.au, various social media channels (including LinkedIn, Facebook and Twitter), email groups, and digital newsletters to communicate with the public.

If we take photos, videos or screenshots of individuals or groups to document and promote our activities, we want to ensure that these images are collected and used in accordance with people's

expectations or wishes. Therefore, we have procedures and other guidance for our Staff to ensure that our use of photography is always respectful and responsible.

From time-to-time we conduct surveys about land development and housing needs. Surveys are conducted with as much anonymity for participants as possible. We collect email addresses of survey participants to issue follow-up invitations for further surveys, and to notify participants of any prize they've won (if that survey involved a competition). Responses to survey questions (including those relating to demographic information or opinions) are separated from email addresses so that they cannot be linked to individuals. We may share non-identifying stakeholder engagement 'outcomes data' with our project partners, including state and local government agencies and industry partners. We may also share research data with research collaborators including universities, state and local government, and industry.

4.2 Our management of enquiries, feedback, complaints and compliments

We want to provide fast and easy ways for people to approach us or provide us with feedback to enable the public to communicate with us regularly through a number of channels.

We receive a range of diverse enquiries, complaints and compliments through links on our website, emails, letters, phone calls and social media. Staff can report any Health Safety & Environment-related hazards or incidents through our HSE system. In the future, the HSE system will allow any person at a Landcom site to report a HSE concern or matter. All feedback, complaints and compliments are dealt with confidentially and personal information is managed in accordance with this PMP and other relevant policies.

We also want to ensure that sensitive matters can be reported through the right channels. Accordingly, our feedback process is designed to encourage the public not to use the main info@lancom.nsw.com.au channel to make a privacy complaint, but rather convey their complaint directly to relevant Staff, including to our Privacy Officer. Reports about legal or integrity concerns can also be lodged through our externally managed 'Speaking up' Integrity Hotline platform.

4.3 Our property reservations, sales and conveyancing work

In delivering land sales or housing to the public, we collect personal information at three stages:

1. Our Sales and Marketing staff collect basic personal and demographic information from people who express interest in a land development site or project;
2. Our Sales and Marketing staff also collect similar information, together with a non-refundable reservation fee from people who wish to reserve land that is publicly released; and
3. Our in-house Legal team uses the personal information collected in Stage 2 and discloses it to other relevant parties as needed to complete a sale and conveyance of property.

4.4 Other functions common to NSW public sector agencies

We carry out a range of functions common to other NSW government agencies. These include:

- Recruitment and staff management;
- Health Safety and Environment Management;
- Finance and IT management;

- Policy and strategy development and project management;
- Audit and risk management; and
- Management of contracts and agreements for other services that we use Suppliers to carry out for us. We may contract directly with third-party suppliers for additional technology support, development, construction, property or research-related projects, or audits to be completed or run on our behalf.

Sections 5 and 6 of this PMP set out further details about *how* we collect, use, share and store personal and health information.

Section 7 sets out how we apply the enforceable NSW Privacy Principles in this every-day work.

4.5 Other relevant matters

Landcom partners with the public and private sector via memorandums of understanding and other contractual arrangements to fulfill our functions and deliver on strategic and complex development projects on vacant or established sites. We ensure that the limited personal information relevant to these arrangements is handled in accordance with the IPPs and HPPS. We do not enter into referral arrangements involving personal information with other private or public sector organisations.

5 How we collect personal and health information

5.1 The main types of personal and health information we collect

We collect information about purchasers, members of the public, and other stakeholders via a range of channels, including web forms, online engagement, participation at events, surveys and research, visits to sales offices, info@emails or phone calls, and through use of 'Google Analytics' web browsing software.

Depending on the nature of our dealing, the types of personal and health information we may collect may include:

- For our Staff, we collect name, date of birth, citizenship, ethnic background, gender, driver's licence number or other identification, (to verify identity, including for employment management) and evidence of relevant qualifications or experience). It is our policy to sight identification, such as drivers' licences and not make or retain copies wherever possible;
- For our purchasers, we collect name, address and contact details. It is our policy that we ask to sight identification, such as drivers' licences (to verify identity as required for property conveyances) but we do not make or retain a copy;
- Records of the products, information and services we have provided to customers and stakeholders;
- Demographic and opinion-related information relating to our projects, including opinion on our projects, housing types and/or housing needs to improve our projects or to better inform the effectiveness of our policies, targets, and strategies;
- Information collected from public sources – media sites, social media channels, subscription services and professional social networking sites such as LinkedIn;

- Photographic images (taken to document or publicly promote our community and industry based events, projects and other activities);
- Training certificates, licences and certificates of competency for workers (if required for compliance purposes);
- Workplace Health and Safety records, incident reports or other integrity-related matters;
- Health information (such medical certificates, disclosures of pre-existing medical conditions, or other medical reports for Staff); and
- Complaints, compliments, enquiries, testimonials and other types of feedback.

5.2 The main ways we collect personal and health information

5.2.1 Information that you give us directly

We may ask you to provide us with specific personal or health information if you are seeking a particular service or product from us. This might happen over the telephone, through a form on our website, by filling in a paper form, or meeting with us face-to-face.

You might also provide your personal or health information to us, without us directly asking for it – for example, if you choose to engage with us on social media.

Please see Section 7 for more information on how we apply the NSW Privacy Principles.

5.2.2 Information that we collect from other parties

When managing land sales, we may collect personal information from official sources to give effect to a legal conveyance of the land.

If you apply for a job or contract with us, we will collect personal and/or health information about you, including from your referees with your consent. We may also conduct other checks on suitability for the role or contract via other third parties. Depending on the role type, these may include conducting a National Police Check, verification of past academic or work history, or a professional qualification from a university, bankruptcy or other background checks. Section 5.3 sets out more information about our management of recruitment and employment information.

We may also check some details about our contractors, consultants and suppliers from publicly available sources, such as the Australian Business Register, NSW Fair Trading and Australian Securities & Investment Commission databases.

5.2.3 Information that we generate ourselves

We maintain records of the interactions we have with land purchasers and the members of the public with whom we interact, including records of products and services we've provided. We also produce reports about our engagement with the public to document the community views we receive about our projects.

We collect limited information about users of our websites, for diagnostic and analytic purposes. We use cookies to collect internet protocol (IP) addresses, but we do not trace these back to individual users.

The information collected during each website visit is aggregated with similar logged information to identify general patterns of usage of our websites. This assists us to improve our websites and the services offered through them. More information about our website analytics is set out in our Privacy Statement on the Landcom website.

5.3 Further information on management of recruitment and employment

From the start of recruitment, we, or a recruitment agency collect information directly and voluntarily from candidates applying for a role, with indirect collection via other parties (such as those used to complete background checks) only taking place after a candidate has been shortlisted for a role. We will never ask for more personal information than that required for the specific recruitment-related purpose and will only do so with consent when it's required. Unless required, we will usually ask to sight the information and not retain a copy.

We may occasionally collect or be supplied with health information during recruitment. If a candidate indicates that they have a health condition that may affect their ability to perform some aspects of the job, this would be a supply of 'health information'. In most cases when this occurs, our process requires us to sight the health information and not retain a copy.

Throughout employment, we collect, access and use information (including personal and/or health information) from and about our Staff for various reasons. These include for:

- Managing staff access to our systems, including individual on-boarding and off-boarding for email and other secured databases;
- Payroll and leave management;
- Individual learning, development and performance reviews;
- Workforce planning;
- Workplace health and safety and return to work requirements (e.g. health information may be collected to put reasonable adjustments in place, manage some forms of leave, or deal with workplace injury or illness); and/or
- Managing any conflicts of interest or other conduct concerns, so that we can operate with transparency and integrity.

Over the course of employment or engagement, we may also take photos of Staff to document Landcom activities, such as training or community events and often use these in corporate publications.

Staff can input and change some information themselves in our Employment Self Service (ESS) system. For example, although we don't currently collect information about people's cultural identity at the recruitment stage, Staff may volunteer this information during employment and can help us to collect statistical data to support culturally inclusive employment at a whole-of-organisation level, and to meet the goals of our Diversity and Inclusion Policy and Action Plans.

All employment-related records are held centrally in electronic files accessed and managed by the People & Culture team. Records are accessed by specific People & Culture staff or relevant

People Managers strictly as needed for employment-related functions. Some records, such as recruitment-related records or learning and development records will at times be managed within an individual operating area, but with longer term storage and retention in accordance with our *State Records Act 1998 (NSW)* obligations.

Records are securely retained until they can legally be destroyed in accordance with specific procedures made under the *State Records Act 1998 (NSW)*.

Some People & Culture practices that involve the collection, use and disclosure of personal and health information are governed by other laws in addition to privacy laws. They include the:

- Government Sector Employment Act 2013 (NSW);
- Federal Income Taxation law, Migration Act 1988 (Cth) and the Child Support (Registration and Collection) Act 1988 (Cth);
- Industrial Relations Act 1996 (Cth);
- Work Health and Safety Act 2011 (NSW); and
- Workers Compensation Act 1987 (NSW).

6 How we handle personal and health information

This section of the PMP summarises the NSW Privacy Principles Landcom must follow and how we handle personal and health information in line with them, using examples from some of our functions.

The PPIP Act and HRIP Act outline principles for managing personal and health information. There are 12 Information Protection Principles (IPPs) outlined in the PPIP Act and 15 Health Privacy Principles (HPPs) in the HRIP Act.

The principles apply to all NSW agencies and regulate the collection, storage, use and disclosure of personal and health information.

6.1 IPP 1 and HPP 1: Collection must be for a lawful purpose

These Principles require Landcom to collect personal and health information only if:

- It is for a lawful purpose that is directly related to one of our functions; and
- It is reasonably necessary for us to have the information.

HPP 1 also states that health information must not be collected in an unlawful way.

How we apply these Privacy Principles

We won't collect personal information unless it is directly related to the function or activity our Staff are performing. As examples:

- When collecting contact information for a person who indicated they would like to receive one of our newsletters, we only use that information to send out the newsletter in accordance with the person's subscription preferences;

- When processing a legal conveyance of property, we use standard conveyancing practices and limit the information we collect to only that needed to complete the sale and as required by legislation.

We take steps to avoid collecting personal information we don't need wherever possible. For example, our Staff can anonymously:

- Participate in regular surveys about workplace experience; or
- Report a complaint or serious conduct concern (although we may be limited in our ability to act on some anonymous complaints, and certain protections are afforded to both Staff and some contractors under the *Public Interest Disclosures Act 2022* (NSW)).

6.2 IPP 2 and HPP 3: Collection directly from the person the information is about

These principles state that:

- Personal and health information must only be collected directly from the individual the information is about, or someone they've authorised to provide it;
- A parent or guardian can provide personal information about their child, if under 16 years, and
- Health information should be collected directly as well, unless impracticable or unreasonable.

How we apply these Privacy Principles

In most cases, we collect personal information from the individual concerned to supply a service of some kind or as part of an application. When we collect information from third parties, it's generally to verify significant components, with prior consent (e.g. a criminal record check conducted for recruitment purposes) or as required by law (e.g. a report of a HSE incident).

We don't generally collect identifying information about children for our functions. At the most, we may collect 'group shots' of children attending a community event with a parent or guardian. We avoid taking photos or videos of people at our events if it is their preference to not be photographed or filmed. We have clear, documented processes designed to ensure that collection of information occurs in the most respectful and appropriate way.

6.3 IPP 3 and HPP 4: Notification when collecting information

These principles require us to take reasonable steps to ensure that before we collect personal or health information, or if not before, then as soon as practicable after, we will tell you:

- The fact that we've collected it;
- The purposes for which we've collected it;
- The intended recipients;
- Whether you must give it to us by law, or if this is voluntary, and any consequences for you if the information isn't provided;
- Your rights to access or correct it; and
- Our name and address as the agency collecting the information and who will ultimately hold it.

If we collect health information from another person, we need to take these steps as well.

How we apply these Privacy Principles

We ensure that all written or digital forms we use to collect personal or health information include collection statements to explain or reference the above matters, as needed in the context.

When our Staff collect information orally, such as at a community event, they are also expected to explain the above information, as the context requires. Some of our policies and charters implicitly describe how we will manage personal information for our functions. Key examples are the Community Participation Plan (for relevant planning assessments under Division 5.1 of the EP&A Act), the Etiquette Guide and Moderation Policy (for management of online discussion forums), the Join-in – Engagement Charter and the Social Media Terms of Use.

6.4 IPP 4 and HPP 2: Collecting high quality information

When we collect personal and health information, we need to take reasonable steps to ensure it is:

- Relevant, accurate, up-to-date and complete; and
- Not unreasonably intrusive or excessive.

How we apply these Privacy Principles

We recognise that having high quality, accurate and up-to-date records is essential for good decision making on our projects, and to be able to deliver the local infrastructure that new communities need to grow and thrive. To do this, we:

- Design our community engagement and feedback mechanisms in a way that enables us to build an understanding of community needs, and reflect them in our development projects without being unreasonably intrusive or excessive. This is ensured through the resources made to staff via Landcom's Privacy Framework;
- Implement processes to ensure that the limited health information we collect is relevant to the purpose for which it is being collected, not excessive or unreasonably intrusive;
- Give careful consideration to determining which organisations, and which records are the best and most reliable sources of information to use in our work; and
- Educate our staff on high quality data collection practices.

6.5 IPP 5 and HPP 5: Security and storage of information

We use a full range of procedures and security measures to ensure the personal and health information we hold is used responsibly, stored securely, not kept longer than necessary, and disposed of appropriately. Our security obligations arise whenever we hold personal or health information (either for the records we create or receive, or through staff access to systems and databases). In particular, we must:

- Ensure personal and health information is kept no longer than necessary for the purposes it can be used or legally required to be kept;
- Dispose of it securely and in line with any requirements for retention and disposal (generally, as issued by the State Archives and Records Authority under the *State Records Act 1998 (NSW)*;
- Use reasonable safeguards to protect the information against loss, unauthorised access; misuse, modification or disclosure; and

- If providing access to or giving personal information to one of our own Suppliers, take reasonable steps to prevent unauthorised use or disclosure of the information.

How we apply these Privacy Principles

Landcom-wide information governance

In recognition of the importance of good governance across the organisation, we have established processes to lead the development and implementation of our governance framework. We also have an Audit & Risk Management Committee which assists our Board in accordance with the Audit and Risk Management Committee Charter.

Our Audit & Risk Management Committee Charter outlines our approach to, and arrangements for managing risk. The role of this Committee includes oversight and review of the effectiveness of compliance with applicable legislation, including NSW Privacy Laws.

Landcom also considers and applies the privacy compliance advice of our Privacy Officer and Legal team when implementing new information management systems and software, to ensure these systems comply with the PPIP Act and HRIP Act. All relevant new information management systems and software engagements or other types of engagements with Suppliers that involve the handling of personal information are subjected to a Privacy Impact Assessment (PIA).

Cyber-security

We actively monitor and manage cyber-risks in line with the NSW Cyber-security Policy. Risks to our information and systems are routinely assessed using independent, external security systems to validate specific controls, integrity of systems and effectiveness of security processes.

We also have a Data Breach Response Plan, as required by the PPIP Act to guide our actions should notifiable data breaches of personal or health information occur.

We train our Staff on cyber-security and regularly remind them to be especially vigilant about the risks to data security posed by external threats such as email phishing scams.

Enforcing appropriate use of personal and health information

All Staff are required to comply with our Staff Code of Conduct and our Suppliers are required to comply with a Supplier Code of Conduct in addition to other contractual terms that protect privacy.

The PPIP Act has provisions for prosecuting individuals for unlawful disclosure of personal information. Section 308H of the *Crimes Act 1900 (NSW)* also makes it an offence to gain unauthorised access to, or to modify restricted records held in a computer. Any unlawful access to information by our Staff would result in disciplinary action, and in serious cases, termination, referral to other agencies or police for criminal prosecution.

Specific security controls we employ

We employ other technical, operational and physical security measures to protect our records, which include, but are not limited to the following:

- Password-protected access to our systems (including two-factor authentication for system access via portable devices);
- Access to specific working files is limited to individuals or individual work groups to ensure that only relevant staff have access to information based on their role and need; and
- Regular audits are undertaken to ensure the right access has been given to the right people.

We comply with the retention and destruction requirements of the *State Records Act 1998 (NSW)*.

The records we create or receive have different retention periods, depending on the use for which they were created or received. Accordingly, we have specific, built-in retention requirements for the electronic document and records management system used to manage our corporate records.

Records managed by our Suppliers

When we use another party to provide services on our behalf, we ensure a range of privacy-protective provisions are included in their contract, where appropriate. This includes an obligation to comply with privacy laws, inform Landcom of data breaches and maintain an appropriate standard of cyber hygiene.

6.6 IPP 6 and HPP 6: Transparency of our information management

These Principles require us to take reasonable steps to enable people to find out:

- Whether we hold personal or health information, generally;
- Whether we hold information relating to an individual (who asks), and if so:
  - The nature of the personal or health information;
  - The main purposes for which it is used; and
  - The individual's entitlement to access it.

How we apply these Privacy Principles

- The publication of this PMP on our website and regular communication to Staff help us to achieve transparency in respect to information handling.
- We issue reminders to Staff that these privacy obligations are broad and are not necessarily achieved merely by giving privacy collection statements on forms, or during direct interaction with people when we collect personal information.

6.7 IPP 7 and HPP 7: Access to information we hold

These Privacy Principles confirm that anyone has the right to request access to the personal or health information Landcom holds about them, and that access must be provided without excessive delay or expense.

You can make enquiries at any time to find out if Landcom holds personal or health information about you and, once we have confirmed your identity, you will be provided with access to your personal or health information unless we are authorised or required by law to refuse access. If requested, we will provide written reasons for any refusal in line with our commitment to transparency. Access requests can also be made under the *Government Information (Public Access) Act 2009 (NSW)* (GIPA Act).

How we apply these Privacy Principles

If you want a copy of personal or health information we hold, or as held by one of our Suppliers on our behalf, we will usually be able to be provide the information to you, free of charge. In some cases, you may need to make a formal access application under the GIPA Act – for example, if your personnel file or your personal information contains the personal information of others.

If you are having difficulty accessing your personal or health information, or you wish to make a formal application, you can email the Right to Information and Privacy Officer: right2info@landcom.nsw.gov.au or privacy@landcom.nsw.gov.au.

6.8 IPP 8 and HPP 8: Correction of information we hold

These Privacy Principles state that if an individual requests an amendment to personal or health information we hold that relates to them, Landcom must:

- Make amendments (e.g. by correcting, deleting or adding information) to ensure it is accurate, relevant, up-to-date, complete and not misleading;
- If not prepared to amend the information, take reasonable steps to allow the individual to associate a clarifying statement with it; and
- Where practicable, notify any recipients of that information of the amendments made.

How we apply these Privacy Principles

Once we have confirmed your identity, you may ask to update or amend personal or health information we hold, to ensure it is accurate, relevant, up-to-date, complete and not misleading. Staff can make basic updates to their records themselves through our Employment Self Service (ESS) system.

In some cases, your request and proposed corrections will need to be in writing. This is so we can verify your identity as well as keep a reliable record of the correction.

We may need to verify the accuracy of the information you would like to be amended, e.g. by confirming the information with its original source. If you don't know which division within Landcom to direct your request, or if you are having difficulties amending your personal or health information or wish to make a formal application to amend records, please email the Privacy Officer at privacy@landcom.nsw.gov.au and ask for your personal information to be amended.

If you are unsuccessful in amending your personal or health information, you can request a formal process known as an 'internal review'. Please see section 7.2.1 of this PMP for more information on the internal review process and how to request one.

6.9 IPP 9 and HPP 9: Accuracy of information

These Privacy Principles state that Landcom must not use personal or health information without taking reasonable steps to ensure it is relevant, accurate, up-to-date, complete and not misleading.

How we apply these Privacy Principles

Our Staff ensure the accuracy and relevance of information they use by always managing it in the official systems intended and designated for this use. This gives Staff a 'single source of truth' for information, the means to readily retrieve it, and the confidence that it is reliable for decision making.

We also ensure accuracy of information by:

- Collecting it directly from individuals (as the primary source) wherever practicable;
- Giving notice of the purposes to which the information will be put (so that people understand the importance of it being accurate, complete and up-to-date, and the consequences if it is not);
- Properly authenticating identity – so that the correct records and any updates are attributed to the correct people; and
- Making access and correction of personal information easy so our records are of high quality.

Landcom may consider the following to determine what 'reasonable steps' are required to ensure personal or health information is relevant, accurate, up-to-date, complete and not misleading:

- The context in which the information was obtained;
- The purpose for which we want to use the information;
- The potential effects for you as an individual if the information is inaccurate or irrelevant;
- Any opportunities we've already given you to correct inaccuracies; and
- The effort and cost in checking the information.

6.10 IPP 10 and HPP 10: How we use personal and health information

These Privacy Principles state that Landcom can use personal or health information only for the purpose it was collected, or for other limited permitted uses described in the Privacy Principles. These other permitted uses include:

- Uses that have the individual's consent;
- Uses that are directly related to the original purpose for which the information was collected (and if health information is involved, would be reasonably expected);
- Use as necessary to lessen or prevent a serious and imminent threat to life or health of the individual or another person (or if health information is involved, to deal with a serious threat to public health or safety); and
- If health information is involved, use to assist in an emergency, where seeking consent is impracticable or unreasonable;

Please note that 'using' information is different to 'disclosing' or 'sharing' it with others. Our Staff use information when we work with it internally within Landcom, including when we update it, migrate it to a new system, de-identify or assemble it for any statistical analysis, modify it in some other way, or arrange to have it archived. Landcom may also use personal information when we share or transfer it to a third party data hosting provider who simply holds the data and acts according to our instructions.

How we apply these Privacy Principles

In most cases, Landcom will only use personal and health information for the actual purpose it was collected, with any planned secondary purposes outlined in a collection statement. Two examples of directly related secondary uses of personal information are:

- Staff de-identifying records to produce reports for Landcom's Shareholder Ministers;
- An auditor working for Landcom who accesses and uses records as needed to ensure Landcom is meeting its legal compliance obligations.

Using statistical information

We will use statistical information (e.g. from website analytics or from surveys) that may be based on personal information gathered from a variety of documents – for analysis, strategy formulation, and planning new projects. This information is de-identified or aggregated so that no individual can be easily recognised.

Both the PPIP Act and HRIP Act allow us to not comply with these Privacy Principles in some cases. See section 6.13 'Exemptions from compliance with IPPs and HPPs'.

6.11 IPP 11 and HPP 11: How we disclose personal and health information

'Disclosing' personal information means sharing it with, or giving access to external parties who are not Landcom Staff. This may include where we share personal information with a third-party contractor we have engaged to perform services on our behalf in order to carry out our functions. IPP 11 states that Landcom must not disclose personal information to another person or body unless:

- The disclosure is directly related to the purpose for which the information was collected, and there is no reason to believe that the individual would object;
- The individual is reasonably likely to have been aware that information of that kind is usually disclosed to the other person or body; or
- Staff reasonably believe that the disclosure is necessary to prevent or lesson a serious and imminent threat to the life or health of the individual or another person.

HPP 11 states that Landcom must not disclose health information to another person or body unless this is for the purpose the information was collected, or:

- With consent;
- If directly related to the original purpose, and reasonably expected;
- To assist in an emergency, where seeking consent is impracticable or unreasonable;
- To lessen or prevent a serious and imminent threat to life, health or safety of the individual; or another person, or a threat to public health or safety.

HPP 11 permits disclosure of health information for other purposes, but those are not likely to apply to Landcom.

Additional obligations arise if the information is:

- 'Sensitive' (about ethnic or racial origin, political opinions, religious or philosophical beliefs, trade union membership or sexual activities); or
- Disclosed to a person or body outside of NSW, or to a Commonwealth agency.

See section 6.12 'IPP 12 and HPP 14: Stricter rules apply for some disclosures.

How we apply these Privacy Principles

Our general approach to compliance with the *disclosure-related* obligations is the same as when our Staff *use* personal information. In most cases, Landcom discloses personal and health information only for the primary purpose it was collected, or a directly related and reasonably expected secondary purpose. Other cases where Landcom might disclose personal information include:

- Disclosure with an individual's formal, written consent, which would permit a person's name and photo taken at a local community event to be included in a corporate publication like our annual report or shared with a project partner;
- Disclosure of personal information for which individuals are reasonably likely to have been told is 'usual', for example:
  - Regular submission of Staff salary information to the Australian Taxation Office and chosen superannuation fund;
  - When an individual purchases land, information about them is disclosed to external bodies to complete the sale.

Both the PPIP Act and HRIP Act allow us to not comply with these Privacy Principles in some circumstances. See section 6.13 'Exemptions from compliance with IPPs and HPPs'.

6.12 HPP 12 Identifiers

This Health Privacy Principle requires agencies to only identify people by using unique identifiers if it is reasonably necessary to carry out our functions efficiently in respect to health information.

How we apply this Privacy Principle

In carrying out our functions, Landcom does not use unique identifiers to identify individuals in respect to health information.

6.13 HPP 13 Anonymity

Wherever it is lawful and practicable, individuals are to be given the opportunity to not identify themselves when entering transactions with or receiving health services from Landcom.

How we apply this Privacy Principle

While Landcom does not provide health services in the ordinary course of business, staff are able to remain anonymous when accessing Landcom's employment assistance program or certain other health related services made available to them through their employment.

6.14 IPP 12 and HPP 14: Stricter rules apply for some disclosures

Certain types of personal information are given additional protection under privacy laws, due to their sensitive nature. This is information about an individual's:

- Ethnic or racial origin;
- Political opinions;
- Religious or philosophical beliefs;
- Trade union membership; or

- Sexual activities.

IPP 12 requires Landcom to not disclose this protected information without consent unless it's necessary to prevent a serious and imminent threat to life or health of the individual, or another person.

How we apply this Privacy Principle

There are very few circumstances where we collect protected information for our functions. This means that there are limited circumstances where it would be disclosed. But one example would be where we invite a respected First Nations community member to hold a ceremonial role at a public launch, and then with their consent, document details of the role they played in a published report.

In addition, disclosing any personal or health information to someone outside of NSW, or to a Commonwealth agency, is only permitted in limited circumstances, as set out in IPP 12 and HPP 14. They include:

- Where staff reasonably believe that the recipient is subject to binding requirements that are substantially similar to the IPPs or HPPs;
- Where reasonable steps have been taken to ensure that the information will not be held, used or disclosed by the recipient inconsistently with the IPPs or HPPs; or
- If permitted or required by an Act or any other law (including Commonwealth, State, or local laws, and court orders).

How we apply these Privacy Principles

Our functions mostly do not usually involve disclosure of personal or health information outside of NSW. But, for our Staff management functions, we share personal information with Commonwealth government as required by law. An example of routine disclosure outside of NSW would be payroll information to the ATO. An example of a non-routine disclosure might be our response to a statutory request, or to Fair Work in response to a court order, where we would be required to disclose personal or health information by law.

While some of our third-party data hosting and storage occurs outside of NSW, these contracts have robust measures which impose obligations on the third-party data hosting and storage suppliers to protect the privacy and security of this information, including obligations to comply with relevant privacy laws, maintain an appropriate level of cyber hygiene and notify Landcom in the event of a cyber breach.

6.15 HPP15 Linkage of health records

Under this Health Privacy Principle, agencies can only add a person to a health records linkage systems if the person has consented.

How we apply this Privacy Principles

This Health Privacy Principle is not applicable to Landcom as our functions do not require us to access or use health records linkage systems.

6.16 Exemptions from compliance with IPPs and HPPs in some cases

Some IPPs and HPPs do not apply in certain situations, or to certain information Landcom holds. Examples of situations where collection, use or disclosure of information is exempted from compliance with certain IPPs and HPPs include:

- For unsolicited information, unless we have elected to retain and use it for our functions;
- To assist law enforcement and investigative agencies (e.g. police);
- To protect public revenue;
- Some complaints handling purposes;
- When authorised or required by a court order, warrant or statutory notice, such as a Standing Order 52, to produce;
- If another law authorises or requires us to not comply, such as the *Government Information (Public Access) Act 2009*, *State Records Act 1998* or the *Public Interest Disclosure Act 2022*;
- In the case of health information, to lessen or prevent a serious threat to public health or safety;
- Where there are any codes of practice or public interest directions relevant to Landcom which provide an exemption. There are currently no codes of practice or public interest directions that are likely to affect how Landcom manages personal information;
- Some research activities, where specific requirements to protect privacy are met; and
- Where information is sent between public sector agencies to transfer enquiries (e.g. to manage a person's correspondence to a Minister).

We aim to handle personal and health information consistently with IPPs and HPPs without having to rely on an exemption wherever possible – that is, by collecting, using and disclosing personal information with individuals' consent, or in line with their reasonable expectations.

6.17 Dealing with data breaches

A data breach occurs if personal or health information is lost or accessed or disclosed without authority. Some examples of data breaches include:

- Accidental loss or theft of information or equipment on which information is stored;
- Accidental or unauthorised disclosure of personal information (e.g. in an email sent to an incorrect recipient); and
- Unauthorised access to information, or systems that hold information, by way of malicious behaviour, phishing attacks, or malware.

The PPIP Act requires all NSW Government agencies to manage data breaches in line with a new *Mandatory Notifiable Data Breach Scheme*. Under this scheme Landcom must:

- Immediately take all reasonable efforts to contain a data breach once it's been identified;
- Undertake an assessment within 30 days, where there are reasonable grounds to suspect there may have been an 'eligible data breach' (one that is likely to result in serious harm);
- Make all reasonable attempts to mitigate the harm done by the suspected breach;
- Decide whether a breach is an eligible data breach or there are reasonable grounds to believe it's an eligible data breach;
- Notify the IPC and (with few exceptions) affected individuals of the eligible data breach; and
- Comply with other recordkeeping requirements.

If you believe that a data breach may have occurred, please advise Landcom's Privacy Officer without delay at privacy@landcom.nsw.gov.au or call (02) 9841 8626. Landcom will follow a specific process to manage any breach in line with the PPIP Act, our published Data Breach Policy, and any other steps the IPC may require or recommend.

7 Your rights

7.1 How to access and/or amend your persona or health information

Everyone has a right to access or amend personal and heath information held about them. Please note that this is a right to access existing documents and records containing personal or health information held by Landcom (meaning information it has in its possession, or a legal right to access). This should be distinguished from the right to obtain answers to specific questions (e.g. "Can you tell me whether you plan to…?").

These rights are subject to some exceptions – for example if giving you access might impact on the privacy of another person. Unless an exception applies, if you request access to your personal information, we must give you access within a reasonable time and without unreasonable expense.

7.1.1 Informal application to access / amend your information

We attempt to give access to personal information informally wherever possible, so long as we can verify your identity. In most instances there will be no charge to access your information. To seek access to, or correction of, your personal information or health information, please contact our Privacy Officer at privacy@landcom.nsw.gov.au.

7.1.2 Formal application to access / amend your information

You also have the right to make a formal access application to access information under the GIPA Act. The GIPA Act sets out the legal exemptions that may apply, but also gives you a right of internal and external review. You can make a formal application at any time, without first making an informal request.

If you wish to make a formal access application under the GIPA Act, more information is available on Your Right to Information on Landcom's website, including Landcom's Access Application form. Alternatively, please contact the Right to Information Officer on right2info@landcom.nsw.gov.au.

7.1.3 Accessing or amending another person's information

The PPIP Act and the HRIP Act give people the right to access their own information – not someone else's. However, the PPIP Act allows Landcom to provide a third party with an individual's information when that individual's consents to this. Similarly, the HRIP Act, enables an 'authorised person' to act on behalf of someone else. Examples of authorisations include a lawyer acting for an individual.

7.2 Your right to raise a privacy concern or complaint, or seek review

People can make privacy complaints about Landcom's compliance with the IPPs and HPPs. We welcome the opportunity to discuss any privacy issues you may have as, sometimes, a fuller

explanation about a particular process or a necessary disclosure can improve transparency and understanding which may be enough to resolve a complaint.

You can also raise a privacy concern, question or complaint by contacting Landcom's Privacy Officer at privacy@landcom.nsw.gov.au as the issue may be able to be resolved informally or via an alternative complaint process.

The IPC can also receive complaints or provide advice about alleged breaches of privacy. Contact:

> Information and Privacy Commission
> Level 15, McKell Building, 2-24 Rawson Place, Haymarket NSW 2000, or
> GPO Box 7011, Sydney NSW 2001
> Phone: 1800 472 679 Email: ipcinfo@ipc.nsw.gov.au

7.2.1 Internal Review

If you believe Landcom has breached the PPIP Act or HRIP Act in relation to your personal or health information, you can request a formal process known as an 'internal review'. This is an investigation that Landcom must conduct in line with requirements under Part 5 of the PPIP Act. It involves assessing a complaint and whether the IPPs or HPPs have been complied with, and then communicating the findings and outcome with the applicant.

Applications for an internal review must:

- Be in writing and addressed to the Privacy Officer at privacy@landcom.nsw.gov.au. You may use the
- IPC's internal review application form which has been developed for this purpose, but this is not mandatory. The only requirement is that the internal review request is in writing;
- Be made within six months from the date you first became aware of the conduct or such later date as Landcom allows; and
- Be related to your own personal or health information.

On receipt of the application, the EGM Legal & Compliance or the Privacy Officer will conduct, (or appoint a suitably qualified Reviewing Officer who is not substantially involved in any matter relating to the application to conduct) the internal review. Landcom will complete the internal review as soon as is reasonably practicable. If the review is not completed within 60 days, you are entitled to seek 'external review'.

Landcom will also:

- As the IPC has an oversight role, notify the IPC of an internal review application as soon as practicable after its receipt and may provide the IPC with a copy of it;
- Keep the IPC informed of progress, findings, and proposed action;
- Notify applicants in writing within 14 days of completing the internal review of:
  - The findings of the review;
  - Actions proposed to be taken; and
  - Their right to have their complaint reviewed by the NSW Civil and Administrative Tribunal (NCAT) (an 'external review').

Landcom will follow the IPC's guide, How to handle an Internal Review and Internal Review Checklist for Agencies when conducting an internal review. We are also required to publish non-identifying requests for, and outcomes of, internal reviews in our annual reports.

For more information on the internal review process is available on the IPC's website, including the IPC factsheet Privacy Complaints: Your review rights.

7.2.2 External Review

If you are unhappy with the outcome of an internal review, or do not receive an outcome within 60 days, you have the right to seek an external review by the NSW Civil and Administrative Tribunal (NCAT). You have 28 calendar days from the date of the internal review decision to seek an external review. You must apply directly to NCAT, which has the power to make a binding decision.

To apply for an external review or obtain more information, including current forms and fees, contact:

> NSW Civil and Administrative Tribunal – Administrative and Equal Opportunity Division
> Level 10, John Maddison Tower, 86-90 Goulburn Street, HAYMARKET NSW 1240
> Mail: PO Box K1026, SYDNEY NSW 2000
> Phone: 1300 006 228
> Email: ap@ncat.nsw.gov.au
> http://www.ncat.nsw.gov.au/.

8 Glossary of terms and abbreviations

This PMP uses the following terms and abbreviations, some of which are also used in privacy laws:

- **Agency** – a 'public sector agency', as defined in section 3 of the PPIP Act. For the purposes of this Plan and the PPIP Act, an Agency includes state owned corporations such as Landcom.
- **Board** – the Board of Landcom.
- **CEO –** the Chief Executive Officer of Landcom
- **Collection** – (of personal or health information). Landcom's act of acquiring personal or health information, which can include via a written or online form, an email message, conversation recorded by staff in a system, photograph, or video footage.
- **Disclosure** – (of personal or health information). Landcom's act of revealing, sending or giving access to a third party, personal or health information not previously known to them. This can include confirming or updating information for the third party. Third parties do not include our Staff or the individual to whom the personal or health information relates.
- **ExCo –** means the Executive Committee of Landcom.
- **Exemptions from compliance with IPPs and HPPs** – General, specific and other exemptions provided for in specific Divisions in the PPIP Act and HRIP Act.
- **Functions** – is defined in section 3 of the PPIP Act as including a power, authority or duty.
- **GIPA Act** – *Government Information (Public Access Act 2009 (NSW)*.

- **Health Information** – Information or an opinion about an individual's physical or mental health or disability, or express wishes about future provision of health services, or a health service provided or to be provided to them (See the definition in section 6 of the HRIP Act).
- **HPPs** – Health Privacy Principles in the HRIP Act.
- **HRIP Act** – *Health Records and Information Privacy Act 2002 (NSW)*.
- **Investigative agencies** – Various bodies that conduct work relevant to accountability and oversight, such as the NSW Audit Office, Ombudsman, or the Independent Commission Against Corruption. The PPIP Act lists additional investigative agencies.
- **HSE** – Health, Safety & Environment.
- **IPC** – Information and Privacy Commission, the NSW regulator of both the PPIP Act and HRIP Act.
- **IPPs** – Information Protection Principles in the PPIP Act.
- **Law enforcement agencies** – NSW Police or another state / territory police force, the NSW Crime Commission, the Australian Federal Police, the Australian Crime Commission, the NSW Director of Public Prosecutions or another state / territory / Commonwealth equivalent, NSW Department of Communities and Justice, NSW Sherriff's Office.
- **NCAT –** The NSW Civil and Administrative Tribunal.
- **Personal Information** – as defined in Section 4 of the PPIP Act as 'Information or an opinion (including information or an opinion in a database and whether or not recorded) about an individual whose identity is apparent or can reasonably be ascertained'. Personal information can include documents containing a person's name and contact details, or other information from which it is relatively easy to work out who they are. An individual's photo without their name can be personal information. The definition excludes some types of information such as generally available information, and information about a person's suitability for employment as a public sector official.
- **PIA** – Privacy Impact Assessment – A structured exercise to identify, assess, and control privacy risks of changes to personal information management through new engagements, projects or programs. Landcom has a PIA process for new programs it implements which involves new or changes the way we handle personal information.
- **PMP** – this Privacy Management Plan.
- **PPIP Act** – *Privacy and Personal Information Protection Act 1998 (NSW)*.
- **Privacy obligations** – The IPPs and HPPs as set out in the PPIP Act and HRIP Act, or as they apply in light of an exemption in these privacy laws.
- **Privacy Officer** – Landcom's Privacy Officer, responsible for maintaining this PMP and a range of other privacy management functions.
- **Privacy Principles** – The IPPs set out in the PPIP Act and HPPs set out in the HRIP Act. Privacy Principles set the minimum standards for all agencies. Non-compliance with some Privacy Principles may be allowed for specific activities and circumstances, treated as 'exemptions'.
- **Staff** – includes the Board, the CEO, all permanent and temporary employees and contingent workers engaged by Landcom. The PMP applies to all Staff.
- **Supplier** – means contractors, subcontractors and consultants engaged to complete specific work for or on behalf of Landcom.

Document Control Table

Document information	
Document approver	Chief Executive Officer
Document owner name	EGM Legal & Compliance
Document delegate name/s	Privacy Officer
Document version number	1.0
Document version date	27 November 2023
Document review cycle	Every three years
Next document review date	November 2026
Document location	External use | Landcom.com.au
Document level	2 = CEO approved document

Linked artefacts	
Linked documents	Complaints & Compliments Framework Customer Relationship Management (CRM) Data Retention & Disposal Procedure Data Breach Response Plan Fraud Control and Corruption Prevention Policy Handling Conflicts of Interest Policy ICT Information Security Policy Join-in – Engagement Charter Moderation Policy and Etiquette Guide Public Interest Disclosure Policy Records Governance Policy and Procedure Staff Code of Conduct Supplier Code of Conduct Workplace Surveillance Procedure
Linked legislation	Landcom Corporation Act 2001 Government Information (Public Access) Act 2009 Health Records and Information Privacy Act 2002 Privacy and Personal Information Protection Act 1998 State Records Act 1998 Workplace Surveillance Act 2005
Linked risks	Reputational Operational Regulatory

Revision history			
Version	**Approval date**	**Author**	**Description**
1.0	27/11/2023	Carina Carter	New PMP implemented following amendments to the PPIP Act