



**ACT**  
Government

# MAJOR PROJECTS CANBERRA INFORMATION PRIVACY POLICY

MAJOR PROJECTS CANBERRA

2024

## Document Information

### REVIEW AND APPROVAL

Date approved: 14 March 2024

Approved by: Gillian Geraghty, Director-General

Date effective: 14 March 2024

Review frequency: Annually

### DOCUMENT DETAILS

Content owner: Assistant Director Risk and Compliance

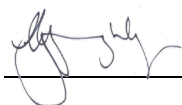
Support Contact: Assistant Director Risk and Compliance  
[MPCGovernance@act.gov.au](mailto:MPCGovernance@act.gov.au)

Objective ID: A5370546

### VERSION CONTROL

Version	Issue Date	Author	Details
0.1	October 2022	Assistant Director, Risk and Compliance	Drafted
0.2	October 2022	Senior Director,	Approved for consultation
0.2	October 2022	Executive Branch Manager, Ministerial, Governance and Corporate Support	Endorsed
0.3	October/November 2022	Corporate and Communications Committee	Endorsed following consultation
0.4	8 December 2022	Consultation with Assistant Director Security and Emergency Management, Senior Director, Corporate Support	Endorsed with feedback incorporated following consultation
1.0	14 March 2024	Director General	Approved

### Approved for implementation by:



**Gillian Geraghty**  
Director General

14 March 2024

**Date**

## Table of Contents

Document Information .....	2
Table of Contents .....	<b>Error! Bookmark not defined.</b>
Table of Contents .....	3
<b>Message from the Director .....</b>	<b>5</b>
<b>1.....About this Privacy Policy .....</b>	<b>6</b>
1.1 What is personal information? .....	<b>Error! Bookmark not defined.</b>
1.2 What is sensitive personal information? .....	<b>Error! Bookmark not defined.</b>
1.3 What is personal health information? .....	<b>Error! Bookmark not defined.</b>
1.4 Anonymity and pseudonyms .....	<b>Error! Bookmark not defined.</b>
<b>2.....The kinds of personal information we collect and hold</b> Error! Bookmark not defined.	
<b>3.....How we collect and hold your personal information ...</b> Error! Bookmark not defined.	
3.1 When will we collect your personal information? .....	<b>Error! Bookmark not defined.</b>
<b>4.....How we collect your personal information.....</b> Error! Bookmark not defined.	
4.1 Confirming your identity .....	11
4.2 With consent.....	11
4.3 Without consent.....	11
4.4 Children and young persons – capacity and consent .....	12
4.5 Secrecy provisions and protected information .....	12
4.6 Data matching.....	13
4.7 Social Networking Services .....	13
4.8 Unsolicited information .....	13
<b>5.....Privacy Noticing.....</b>	<b>14</b>
<b>6.....How we hold, secure and protect your personal information.....</b>	<b>15</b>
<b>7.....Whole-of-Government purposes for which we collect, use and disclose personal information .....</b>	<b>16</b>
<b>8.....Purposes for which MPC collects, holds, uses and discloses personal information.....</b>	<b>17</b>
8.1 Primary Purpose.....	17

---

<b>8.2</b>	<b>Use and Disclosure</b> .....	<b>17</b>
<b>8.3</b>	<b>Disclosure to overseas recipients</b> .....	<b>18</b>
<b>8.4</b>	<b>Use and storage of personal information in offshore clouds</b> .....	<b>18</b>
<b>9.....</b>	<b>How you can access or correct your personal information</b> .....	<b>20</b>
<b>9.1</b>	<b>Access</b> .....	<b>20</b>
<b>9.2</b>	<b>How to request access</b> .....	<b>20</b>
<b>9.3</b>	<b>Are there any charges for access?</b> .....	<b>21</b>
<b>9.4</b>	<b>Correction</b> .....	<b>21</b>
<b>10....</b>	<b>How to make a privacy complaint or report a privacy breach?</b> .....	<b>22</b>
<b>10.1</b>	<b>Making a privacy complaint</b> .....	<b>22</b>
<b>10.2</b>	<b>Privacy data breaches</b> .....	<b>22</b>
<b>10.3</b>	<b>Complaining to the Information Privacy Commissioner</b> .....	<b>22</b>
<b>11....</b>	<b>Contact us</b> .....	<b>24</b>
	Assisted Contact.....	24
	<b>ANNEXURE - DETAILED PURPOSES FOR WHICH MPC COLLECTS, HOLDS, USES AND DISCLOSES PERSONAL INFORMATION</b> .....	<b>26</b>

## MESSAGE FROM THE CHIEF PROJECTS OFFICER

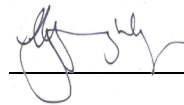
Major Projects Canberra (MPC) was established on 1 July 2019 to lead the procurement and delivery of the Territory's infrastructure program. MPC's purpose is to *build infrastructure that makes Canberra the world's most liveable city*.

To achieve our purpose and meet community expectations, we strive to ensure the way we do business aligns with our legislative and policy obligations and the values of the Australian Capital Territory Public Service.

The ACT has a proud history of protecting and promoting human rights. The *ACT Human Rights Act (2004)* (HRA) was the first bill of rights in Australia to incorporate internationally recognised human rights including those established under the *International Covenant on Civil and Political Rights*. The HRA provides an explicit statutory basis for respecting, protecting and promoting fundamental human rights, including the right to privacy and reputation. The right to privacy underpins the right to autonomy and to decide to whom when and what information we reveal about ourselves.

The *Information Privacy Act 2014* regulates how ACT public sector entities, handle *personal information* so as to safeguard the right to privacy under the HRA in the ACT. MPC is committed to ensuring it meets regulatory compliance best practice with the requirements of the legislation.

The purpose of this policy is to set out the practices, processes, procedures and systems that establish MPC's compliance with the privacy principles contained in the legislation, and to facilitate privacy inquiries, complaints and corrections.



---

**Gillian Geraghty**  
Chief Projects Officer  
Major Projects Canberra  
14 March 2024

## About this Privacy Policy

Major Projects Canberra (MPC) sometimes collects information about individuals. MPC does this only when it is both allowed by law and necessary or directly relevant to the performance of our functions or activities. At all times we try to collect only the information we need to fulfil the particular function or activity we are carrying out. We do not collect personal information about individuals if we do not need it.

The [Information Privacy Act 2014](#) (the Information Privacy Act) is the principal source of the obligations that regulate how ACT public sector agencies handle *personal information*<sup>1</sup>. In particular, the 13 principles (called the Territory Privacy Principles or TPPs) contained in the Information Privacy Act specify how MPC (and other ACT public sector agencies) collects, stores and secures, uses and discloses, corrects and disposes of personal information.

The Information Privacy Act also requires that MPC has:

- a Privacy Notice that explains why we collect an individual's personal information and how we might use or disclose it; and
- a current and up to date Privacy Policy that tells individuals how we will handle personal information when carrying out our functions and activities. This document is our Privacy Policy (refer to TPP 1.3).

MPC's Information Privacy Policy describes:

- What information MPC collects and why;
- Where MPC obtains the personal information it collects;
- How MPC uses, stores, protects discloses and disposes of the personal information it collects.

Importantly, MPC's Information Privacy Policy also describes what you as an individual should do and who you can contact if you want to:

- Make an enquiry about the personal information MPC has about you;
- Correct mistakes there may be in that personal information; or
- Make a complaint regarding MPC's handling of your personal information.

MPC's Privacy Policy will be updated from time to time and updates will be published on the [Major Projects Canberra Directorate Website](#)

## WHAT IS PERSONAL INFORMATION?

The Information Privacy Act defines *personal information* as:

*'information or an opinion about an identified individual, or an individual who is reasonably identifiable— whether the information or opinion is true or not; and whether the information or opinion is recorded in a material form or not'.*

---

**WHAT IS SENSITIVE PERSONAL INFORMATION?**

*Sensitive information* is a subset of personal information that when handled, attracts additional protections. Sensitive personal information can include:

- *racial or ethnic origin*
- *political opinions*
- *religious beliefs or affiliations*
- *criminal record*
- *philosophical beliefs*
- *membership of a political association*
- *membership of a trade union*
- *membership of a professional or trade association*
- *sexual orientation or practices*
- *biometric information (including photographs, video recordings and audio recordings of you)*
- *genetic information.*

For instance, MPC may collect and hold sensitive information about the criminal records of its employees and applicants for employment. This is an ACT Public Service requirement for information that is used to assess an applicant/ employee's suitability to hold a position in the public service.

Sensitive information is handled with additional protections. This includes protecting the security of the information and seeking consent when information collected for a primary purpose will be used or disclosed for an unrelated function or activity (secondary purpose) (unless a permitted exception under the TPPs or law applies). Further, sensitive information that has been collected will only be used and made available to others as allowed by law.

MPC only collects sensitive information when you have consented and the information is reasonably necessary or directly related to one or more of our functions or activities (TPP 3.3). While we will normally seek permission to collect sensitive information, there may be times we collect sensitive information about you without your permission. This might occur when it is required by law, or if it is reasonably necessary to prevent a threat to the life, health or safety of one or more persons.

**WHAT IS PERSONAL HEALTH INFORMATION?**

The [Health Records \(Privacy and Access\) Act 1997](#) defines *personal health information* as:

*'any personal information, whether or not recorded in a health record—relating to the health, an illness or a disability of the consumer; or - collected by a health service provider in relation to the health, an illness or a disability of the consumer.'*<sup>2</sup>

The Health Records (Privacy and Access) Act governs how MPC handles and protects *personal health information* or health records.

This Information Privacy Policy partly covers the requirements of Privacy Principles 2 and 5 of the *Health Records (Privacy and Access) Act 1997*.

## ANONYMITY AND PSEUDONYMS

When dealing with MPC, individuals have the option of remaining anonymous (e.g. when calling to ask for information) or where practical, using a made-up name (or pseudonym) (e.g. when participating in certain online forums) (TPP 2.1).

There may be times when you do need to identify (e.g. by using your real name and other personal details) yourself. This may be because we cannot provide you with help without knowing your name and contact details. Sometimes it may be because MPC is required by law to collect your details or to verify your identity (e.g. applying for a grant or rebate).

If it is impractical or unlawful for us to deal with you without knowing some of your personal information, we will tell you why we need the information. We will also tell you what it will mean for you if you do not provide the information we need. (Refer to TPP2.2)



## MPC's Functions and Activities

MPC was established in July 2019 to lead the procurement and delivery of the Territory's infrastructure program with the aim of providing an economically, environmentally and socially sustainable infrastructure legacy for the Territory.

Our functions and activities include:

- Procuring and delivering infrastructure projects designated by the Chief Minister into Major Projects Canberra;
- Delivering other whole of government infrastructure projects in partnership with other directorates;
- Administration of the ACT Government's Cladding Program;
- Hosting the office of the ACT Chief Engineer whose role it is to provide strategic oversight of infrastructure projects across the Canberra region and support the engineering cohort of the ACT Government;
- MPC also administers schemes for contractor pre-qualification and IRE Certification, project management and reporting, superintendency of works and WHS Active Certification;

Further, ACT Property Group, operating within MPC performs the following functions and activities:

- delivers property and asset management services (including maintenances, upgrades and trade services) to ACT Government owned and leased properties;
- facilitates the provision of properties that house a range of organisations and functions;
- manages Territory owned community venues (including heritage listed venues), aquatic facilities and management contracts involving ACT Government, community and commercial organisations.

The **Annexure** contains more information on the business units within MPC, their functions and the types of personal information they are likely to hold.

## The Information that MPC Collects and Holds

### The kinds of personal information MPC collects and holds

We only collect, hold, use and disclose personal information about you that is reasonably necessary for, or directly related to one or more of MPC's functions services or activities. This is the primary purpose for which personal information is collected and may include but is not limited to:

- Your name address and contact details (e.g. phone email and postal address)
- Information about your identity (e.g. date of birth, passport and visa details, driver's license)
- Information about your personal circumstances (e.g. age, gender, marital status, educational details, occupation, disability, criminal convictions, breaches of conduct)
- Information about your financial and taxation affairs (e.g. payment details, bank account details, superannuation provider, information about business and financial interests)
- Information about your employment (e.g. applications for employment, work history, referee comments, remuneration, registrations and licences held and applied for)
- Information about your opinions (e.g. views, opinions and feedback when engaging with us, submissions on reforms and government policy)
- Information about assistance provided to you and government related identifiers (e.g. tax file number, Centrelink number)
- Photos video or audio recordings.

NOTE: as mentioned above, all health records and personal health information that MPC holds are protected and managed in accordance with the *Health Records (Privacy and Access) Act 1997*.

### How MPC collects and holds personal information

#### WHEN WILL WE COLLECT YOUR PERSONAL INFORMATION

We may collect personal information about you when you

- Send us a letter, fax, email or submit an application;
- Contact us on the phone or through a hotline;
- Fill in one of our online or paper forms;
- Use online platforms to comment and provide feedback, for example YourSay Community Conversations engagement website and the YourSay Community Panel;
- Participate in a meeting or consultation.

MPC may also collect personal information when you:

- Send us a fax, letter, or email or make an inquiry through our "Contact Us" web page (and other contact methods) for information and we need your information to help you or to reply to you;
- speak with one of our staff over the phone or use TTY or TIS services;
- participate in community consultations, committees, forums or make submissions to us and gives us permission to collect personal information;
- enter sites MPC manages as a visitor;
- contract to provide goods or services to MPC;
- participate in recruitment processes in accordance with the *Public Sector Management Act 1994* or become employed by MPC;

- submit an application for certification/ prequalification or registration as an approved supplier contractor or consultant;
- submit a grant or concessional loan application;
- volunteer for a service program or event managed by MPC;
- are involved in an accident incident or near miss related to MPC's activities, resulting in the completion and submission of an incident/accident report;
- participate in procurement processes in accordance with the *Government Procurement Act 2001*;
- request access to information, including under the *Territory Records Act 2002*, or make a Freedom of Information (FOI) request;
- participate in a meeting, consultation or committee or raises a complaint;
- send MPC files or other information that is stored uploaded or provided to us.

## How we collect your personal information

### CONFIRMING YOUR IDENTITY

We are required to verify your identity when:

- we collect your personal information to provide you with specific information or services; or
- we are authorised or required by law to identify you.

We collect the personal information needed to verify your identity and use it to confirm we are dealing with the correct individual.

Sometimes we need to collect and hold the identifying information. Other times, we may only need to 'sight' your identity documents and record the type of identity document and its details. Identifying documents may be a driver's licence, birth certificate, passport, or other acceptable form of identifying personal information.

The ACT Digital Account may also be used to verify your identity. The ACT Digital Account provides users with one account to create a verified digital identity to access and transact with a growing number of ACT Government services.

If you contact us by telephone, and we need to verify your identity to provide you with specific information or a service, we will ask a series of identifying questions. If you choose not to identify yourself (remaining anonymous or using a pseudonym), or where we cannot satisfactorily verify your identity, we may not be able to provide you with some services or information.

### WITH CONSENT

We usually seek your consent when we need to collect your personal and sensitive information for one or more of our functions and activities, or for a directly related purpose.

The law permits us to collect information about you from other person(s) or third parties where:

- you have given your consent to a person or third-party you have authorised to give us the information; and
- you have been given a privacy notice at the time of collection advising you from whom we may collect your personal information, for example:
  - the Executive or other ACT Government directorates;
  - Commonwealth state or territory government agencies, authorities and bodies;
  - Community or not for profit organisations and peak bodies.

## WITHOUT CONSENT

We may collect personal information without your consent where it is reasonably necessary for, or directly related to one or more of our functions and activities. We may also collect your sensitive information without consent from third parties such as other ACT Government directorates, Australian or state/territory governments, and law enforcement agencies or bodies. We will only do this where permitted under the Information Privacy Act, for example, where:

- required or authorised by or under an Australian law, a court or tribunal order; or
- reasonably necessary for or directly related to an enforcement body's functions or activities;
- necessary to prevent a threat to the life, health or safety of one or more individuals, or to public health or safety; or
- another permitted general situation under the TPPs applies.

We may also collect personal information about you without your consent from publicly available sources, such as electoral rolls, newspapers, land titles registers websites and social media platforms like Facebook and Twitter. We may collect sensitive information about you when a member of the public provides information about possible fraudulent or illegal activities.

If we do collect your personal and sensitive information lawfully from a third party without your consent, we will generally advise you of this prior to or at the time of collection. We will not notify you if it is unreasonable to do so, such as during an active fraud investigation.

## Children and young persons – capacity and consent

The Information Privacy Act does not define an age when an individual can make their own privacy decision. When determining whether an individual aged under 18 years of age can provide consent, we refer to the Office of the Australian Information Commissioner (OAIC) guidelines on children, young people and consent.

In general, a person must have the capacity to consent and age is one element that may affect an individual's capacity. Where a child or young person is under the age of 18 years of age, we will generally collect their personal and sensitive information with the consent of their parent(s) or legal guardian(s).

We may accept the consent of a child or young person under the age of 18 if we have assessed the individual as having the capacity to consent. Where it is not possible or practical for us to assess the capacity of individuals on a case-by case basis, we may accept the consent of persons over the age of 15 years unless they are unsure.

When assessing capacity to consent to the handling of their personal information, we consider an individual's age, developmental level, maturity, if they can understand what is being proposed, and if they can form their own views and express those views freely.

## Secrecy provisions and protected information

Laws that have information secrecy provisions may also apply to the personal information that MPC obtains and protects. In general, secrecy provisions place prohibitions, or extra requirements or limitations, on how the information is to be protected and handled. Protected information may also contain personal or sensitive information.

The following are some examples of the kinds of prohibitions that may apply to the information protected by secrecy provisions:

- authorising only certain persons to make a record of, use or disclose the information
- setting limits on the kinds of information or personal information that can be used or disclosed and
- may limit or specify the external or third parties to whom we may lawfully disclose.

Examples of secrecy provisions that MPC is required to comply with, but not limited to include:

- *Taxation Administration Act 1999* – sections 95, 98 and 99;
- *Gambling and Racing Control Act 1999* – sections 34 – 39;
- *Working with Vulnerable People (Background Checking) Act 2011* – section 65; and
- *Road Transport (Third Party Insurance) Act 2008* – section 271.

If an information secrecy provision permits the obtaining of information, the making of a record, or the use and/or disclosure of that information, if that information also contains personal or sensitive information, then that collection, use or disclosure will also be permitted under the Information Privacy Act.

## Data matching

We may collect your personal information using data matching. In general, we use personal information for data matching that has been collected with your consent to confirm the identity of an individual when handling two different sets of data, for compliance or enforcement related functions and activities, or where the law requires or authorises it.

We undertake data matching when providing the following services, function and activities:

- Digital Account- to verify your identity documents using the Document Verification Service(DVS). The DVS' Privacy Statement is available at <https://www.idmatch.gov.au/privacy-security>.

The ACT Government uses DVS to compare your identifying information with a government record to verify your identity. The Digital Account provides individuals with control over who they share their data with on a consent basis.

## Social Networking Services

If you use social media or networking sites like Facebook or Twitter to contact us, we generally will not collect your personal information. If we do collect any personal information about you when you use those sites, we will only collect information which is publicly available, and that is reasonably necessary for, or directly related to one or more of our functions or activities.

Your personal information may also be collected by those social networking services in accordance with their own privacy policies which can be accessed on their websites.

When using our website, you can refer to our [Website Privacy Policy](#) and Privacy - ACT Government for more information about the personal and other information we may collect, store, use and disclose when using our website or online services.

## Unsolicited information

Unsolicited information is personal or sensitive information we receive from a third parties, that we did not ask for. For example, misdirected mail, or complaints that do not relate to our functions or activities.

If we receive unsolicited information, we are required under the TPPs to decide if we could have collected it lawfully. If we decide that we could not have collected it lawfully, we will either destroy the information or de-identify it.

## Privacy Notice

When we collect personal information about you, we are required to take reasonable steps to provide you with a Privacy Notice to tell you more about how we will handle your personal information including:

- who we are and how you can contact us
- if we have collected your personal information from someone else (a third party) and the circumstances of that collection
- if a law authorises or requires the collection of your personal information and the name of that law
- the purposes for which we collect the personal information
- how you may be affected if we cannot collect all or some of the personal information we need
- the details of any agencies or types of agencies to which we usually disclose your personal information
- if we are likely to disclose your personal information to an overseas recipient, and the countries those recipients are in
- where to locate this Privacy Policy, including how you can:
  - access your personal information
  - make a complaint about a breach of your personal information, and how we will deal with that complaint and
  - seek correction of your personal information.

We may provide you with Privacy Notices and policies in a layered fashion. You may be provided with a short notice when completing a paper or online form, or when accessing a portal or communication tools or certain online platforms i.e. YourSay, Digital Account. The short notice will advise you about where to find or locate more detailed information in our Privacy Notice, and in this Privacy Policy.

This Privacy Policy should be read together with MPC's Privacy Notice and any specific privacy notices provided to you when we collect your personal information.

## How we hold, secure and protect your personal information

The Information Privacy Act requires us to take reasonable steps to ensure the personal information we hold is kept safe, secure and protected from misuse, interference or loss and from unauthorised access, use, modification or disclosure.

Key policies and legislation that guide how the Directorate must handle and keep secure the personal information we hold include:

- [ACT Government: ICT Acceptable Use Policy](#)
- [Cyber Security Policy \(act.gov.au\)](#)
- [ACT Government Protective Security Policy Framework](#)
- [Whole of Government Electronic Document and Records Management Systems](#)
- [Territory Records Act 2002](#)

The *Territory Records Act 2002* establishes the framework within which we manage the records of our actions and decisions, which may include personal information. We maintain dedicated record keeping systems to manage both hard copy and digital records. Records, information and data that contain personal information may also be retained in business management and office productivity systems such as revenue management, financial management and case and customer management systems.

We may also be required to protect your personal information under other legislation that imposes additional protections, or where governed by secrecy provisions, for example Tax File Numbers (TFNs).

When we no longer require the personal information we hold, we will take reasonable steps to destroy the information or ensure that it is de-identified, consistent with our obligations under the Information Privacy Act, Territory Records Act and any relevant policies and laws.

## Whole-of-Government purposes for which we collect, use and disclose personal information

The ACT Government has integrated and consolidated many common functions across government to better coordinate and deliver services to the ACT public including procurement, finance, consultative activities, identity verification, and many regulatory services and activities.

The personal and sensitive information collected by MPC or other ACT Government Directorates when carrying out or delivering these functions, services or activities may be accessed, used, or disclosed to or by other ACT Government directorates, the ACT Executive, and contractors who perform various services for and on behalf of the ACT Government.

The purpose of the collection, use and disclosure of personal and sensitive information for those activities is for the *primary purpose* of:

- enhancing customer experiences and outcomes when transacting with the ACT Government by providing a one-stop shop for customer and regulatory services
- enabling lawful and transparent use of data and information sharing across ACT Government to support better communications and engagement with the ACT Government and reduce the effects of over consultation and
- providing a range of Information Communication Technology (ICT), financial and corporate services for the ACT Government and the ACTPS.

Please refer to the ACT Government Open Access website at <https://www.act.gov.au/open-access> for access to other Directorates' policies and information.

Alternatively you may visit <https://www.directory.act.gov.au> for links to all ACT Government Directorates. All Directorates provide links to their own Privacy Policies.



## Purposes for which MPC collects, holds, uses and discloses personal information

### Primary Purpose

The *primary purpose* for which MPC collects, holds and uses personal information, is to be able to effectively carry out our functions and activities or to provide you with services.

Some of the common or primary purposes for which we collect, hold and use your personal information include, but are not limited to:

- Administering the ACT Cladding Program
- Closed Circuit Television (CCTV) for security, monitoring and surveillance
- Corruption, fraud and other prevention activities and investigations
- Compliance and enforcement activities
- Correspondence and communications
- Financial and economic management
- Freedom of Information (FOI) and Territory Records requests
- Quality assurance and internal audit
- Personal Emergency Evacuation Plans
- Personnel information (ACTPS and contractors)
  - Onboarding and ongoing employment
  - Workplace behaviour and conduct matters and
  - Injury and Illness Management
- Prequalification Schemes
- Procurements and tenders
- Project Management and Reporting
- Public Interest Disclosure
- Research
- Security passes and
- Submissions and surveys
- Territory Records (access)

### Use and Disclosure

Some of the permitted secondary purposes we may use or disclose your personal information include where:

- you would reasonably expect us to use the information for the secondary purpose that is related (or directly related – in the case of sensitive information) to the primary purpose for which the information was collected
- the use or disclosure is required or authorised under or by an Australian law, or court order or tribunal
- we reasonably believe the use or disclosure is reasonably necessary for an enforcement body's enforcement related function or activity (i.e. intelligence gathering, surveillance, or monitoring of activities)
- it is unreasonable or impracticable to obtain your consent, and we reasonably believe that use or disclosure is necessary to lessen or prevent a serious threat to the life, health or safety of any individual, or to public health or safety
- we have reason to suspect unlawful activity, or misconduct of a serious nature, that relates to our functions and we reasonably believe that the use or disclosure of the information is necessary for us

to take appropriate action

- we reasonably believe that the use or disclosure is necessary to help locate a person who has been reported as missing; or
- another permitted exception under the Information Privacy Act applies.

For more detailed information about the purposes for which we collect, hold, use and disclose personal information please refer to Annexure – Detailed purposes for which MPC collects, holds, uses and discloses your personal information.

### **Disclosure to overseas recipients**

We do not generally disclose personal information to overseas recipients on a regular basis, or under any international agreements for information exchange.

We will usually obtain your consent in the unlikely event that disclosure to an overseas recipient is necessary. We will also take reasonable steps before disclosing the information, to ensure that the overseas recipient does not breach the TPPs.

Sometimes, we cannot be assured that the overseas recipient will handle your personal information in a similar way to how it is handled under the Information Privacy Act. Where this is the case we will advise you prior to seeking your consent to the disclosure of your personal information to any overseas recipient. Some of the ad hoc business purposes for disclosure to overseas recipients may include:

- to the issuing authorities in your country of former residence or citizenship to confirm the documents you have provided are genuine i.e. checking a motor vehicle licence with the issuing authority of that country, Birth, Death and Marriage certificates where an Apostille or authenticity or certificate and translation has not been provided; and
- International Engagement purposes to support and facilitate stakeholder engagement, and the organisation of foreign missions, delegations and visits.

In limited circumstances, there may be situations where it is impracticable to seek your consent prior to disclosing your personal or sensitive information to an overseas recipient and/or there is a permitted exception to the disclosure under the Information Privacy Act. For example, where the disclosure is reasonably necessary for an activity conducted by an enforcement body, and the recipient is a body that exercises functions similar to those exercised by an enforcement body.

We will update this Information Privacy Policy to reflect any new arrangements that result in the regular or usual disclosure of personal information to overseas recipients.

### **Use and storage of personal information in offshore clouds**

In some circumstances, we may use contractors to provide services on our behalf, including service providers located outside of Australia. Contractors whether in Australia or overseas when handling personal information on our behalf, must comply with the Information Privacy Act and ensure that they do not breach the TPPs.

In some circumstances we or our contractors may need to use and store your personal information in offshore clouds or servers under contracted service arrangements. The use of offshore clouds under such arrangements is not considered a disclosure to an overseas recipient, but a use of that personal information.

We will advise you when collecting your personal information if your personal information will be stored in an offshore cloud and where that cloud is located.

The following programs or services use offshore clouds to store your personal information:

- YourSay – uses Harvest Digital Planning to provide digital platform for the Canberra community to share ideas and provide feedback to the ACT Government on projects and initiatives across Canberra – Harvest Digital Planning’s (the Hive’s) Privacy Policy is available at <https://the-hive.com.au/privacy-policy>
- YourSay Community Panel – uses Vison Critical (*Vision Critical Communications Pty Ltd*) to store personal information in an offshore cloud in servers located in Singapore – Vision Critical’s Privacy Policy is available at: <https://www.visioncritical.com/privacy-policy>
- ACT Government Digital Account- uses Sales Force Software as a Service (SaaS), which is an Australian Signals Directorate (ASD) certified cloud provider – SaaS’s Privacy Policy is available at: <https://www.salesforce.com/au/company/privacy/>; and

Some of our web-based services and tools use overseas providers under contract to provide ICT services, please refer to MPC’s [Website Privacy Notice](#) section for more details.

## How you can access or correct your personal information

### Access

You have the right to ask for (access) your personal information that we hold about you. You can ask in person, over the phone, or in writing. If you ask for access, we will take steps to verify your identity before we will disclose your personal information.

If you have asked another person to access your personal information on your behalf, prior to granting access, we will take steps to verify their identity and confirm they have your consent and authority to receive that information, before disclosing your personal information.

If your personal information is held by a business unit that provides public access or over-the-counter services, you may be able to ask for access in person. However, we have the right to refuse your request where:

- your personal information is not readily accessible, or is contained in a physical file that is stored somewhere else;
- the personal information in your record also contains the personal information of other people or third parties; or
- another law protects or tells us how the information must be disclosed i.e. secrecy laws or laws which require a fee or form that must be used for disclosure.

If we cannot give you access in person, you may be asked to:

- make a written request;
- use or complete an approved form (if one applies including paying any lawful fee); or
  - make an FOI request where there is third party personal information present, or
  - the amount of information is too big for counter staff to process.

If you request access to your personal information, we must provide you with access (in the way you requested if reasonable) within 30 days. If we refuse to provide access, we must advise you in writing (within 30 days of your request) of the reasons for refusal. Reasons for refusal may include where the information is subject to an exemption under the FOI Act, or where disclosure is not permitted under another law.

There are no review rights if we refuse a request for access. You may instead wish to make a request for access under the FOI Act (which does have review rights) or, make a complaint to the Office of the Australian Information Commissioner (OAIC).

Further information about our FOI arrangements, including how you can apply for access, can be found on our [Freedom of Information](#) website.

### How to request access

When requesting access, you should first approach the relevant business unit or relevant officer in the Directorate who you believe may hold your personal information.

Individuals can also request access to, or correction of, their personal information by contacting the Privacy Contact Officer via email to:

Email: [MPCSecurity@act.gov.au](mailto:MPCSecurity@act.gov.au)

Web: [Access to information - Major Projects Canberra \(act.gov.au\)](https://www.act.gov.au)

Mail: MPC Privacy Contact Officer

Major Projects Canberra

GPO Box 158

CANBERRA ACT 2601

Telephone: +61 2 6207 2774

### **Are there any charges for access?**

No, you will not be charged for making the request or accessing your personal information, unless a fee is required by law for the information.

### **Correction**

You can ask us to correct your personal information we hold if you believe it is:

- incorrect;
- out-of-date;
- incomplete;
- irrelevant; or
- misleading.

If you ask us to correct your personal information, we are required to take reasonable steps to do so, if having regard to the purpose for which it was collected, we agree the information is incorrect, out-of-date, incomplete, irrelevant, or misleading.

We may refuse a request to correct your personal information where we believe another applicable law prevents the correction, or if we do not agree that the information is incorrect, out-of-date, incomplete, irrelevant, or misleading.

If we refuse to correct your record, and you ask us to make an associated statement (the statement can say why you believe the personal information is incorrect, out-of-date, incomplete, irrelevant, or misleading), we will do so. We are not required to make an associated statement unless you specifically ask us to make one.

There are no review rights under the Information Privacy Act if we refuse to correct your personal information. You can, however, seek amendment of your personal information under the FOI Act, which does have review rights, or make a complaint to the Australian Information Commissioner (OAIC).

## How to make a privacy complaint or report a privacy breach?

### Making a privacy complaint

If you want to complain about how we handle or have handled your personal information you can phone us. If you phone us however, we will still ask you where it is reasonable to do so, to put your complaint in writing, provide us with your name, address and phone number for contact, and enough information about the business unit or person you are making the complaint about. We can assist you to lodge your complaint if you need help.

We will acknowledge receipt of your complaint within five working days and we will undertake an investigation into your complaint. In general, we aim to have completed our investigation within 21 working days and will endeavour to keep you updated regularly throughout the investigation.

### Privacy data breaches

We take your privacy seriously and will deal promptly with any unauthorised access, use or disclosure of your personal information.

The Office of the Australian Information Commissioner's (OAIC's) Notifiable Data Breaches Scheme (NDBS) does not apply to MPC or other ACT public sector agencies unless the information that is the subject of the breach:

- includes Tax File Numbers (TFN's); or
- personal health information or is part of a health record.

Generally, the NDBS requires agencies to notify individuals whose personal information is involved in a data breach and to notify the OAIC where the breach is likely to result in serious harm to those individuals.

Although we are not required to notify under the NDBS, it is our policy to voluntarily report any significant privacy data breaches to the OAIC. We will seek the OAIC's advice and assistance where we consider a breach may result in serious harm to affected individuals. This aligns with the NDBS and is keeping with best privacy practice.

### Complaining to the Information Privacy Commissioner

You can make a formal privacy complaint to the Information Privacy Commissioner if you do not agree or are not happy with our response to your complaint, or you believe we have breached your privacy.

Under an agreement with the ACT Government, the OAIC performs the role of the Information Privacy Commissioner for the ACT and manages complaints against ACT public sector agencies. The OAIC is an independent body that will assess your complaint and decide if our actions are an interference with your privacy.

Complaints made to the OAIC must be in writing and include your name, address and telephone number, and provide details of the subject of your complaint. Exceptions to this requirement may be made by the OAIC in circumstances where they consider a complaint made by phone appropriate.

The OAIC can be contacted via:

Mail: Director of Privacy Case Management

Office of the Australian Information Commissioner GPO Box 5218

Sydney NSW 2001

Email: [Enquiries@oaic.gov.au](mailto:Enquiries@oaic.gov.au)

Complaints advice and form available at: <https://www.oaic.gov.au/privacy/privacy-complaints/>

Ph: 1300 363 992

If your complaint or alleged breach is upheld by the OAIC and a decision is made, we will comply with any determination made by the OAIC. The OAIC's decision may include remedies such as an apology, compensation, and to undertake actions such as amendment of policies, operations or processes to prevent further or similar interferences with privacy.

## Contact us

If you have any comment or suggestion for improvement in relation to any aspect of the collection, use, security of, or access to your personal information please contact us:

Email: [MPCSecurity@act.gov.au](mailto:MPCSecurity@act.gov.au)

Web: [Major Projects Canberra Access to Information](#)

Mail: MPC Privacy Contact Officer  
Major Projects Canberra  
GPO Box 158  
CANBERRA ACT 2601

Ph: + 61 2 6207 TBC

### ASSISTED CONTACT

If you need assistance when accessing this Privacy Policy, please contact:

#### National Relay Service (NRS)

The NRS is a government initiative that allows people who are deaf, hard of hearing and/or have a speech impairment to make and receive phone calls.

You can access the 24-hour relay call numbers using the links below:



[Make an Internet relay call https://nrschat.nrscall.gov.au/](https://nrschat.nrscall.gov.au/)



[Make a captioned relay call https://nrschat.nrscall.gov.au/](https://nrschat.nrscall.gov.au/)

Speak and Listen number

555 727

TTY number 133 677

SMS relay number 0423 677 767

Other NRS call numbers can be found at: <https://www.communications.gov.au/what-we-do/phone/services-people-disability/accesshub/national-relay-service/service-features/national-relay-service-call-numbers>

Choose the 'Making a call' option that suits your needs to contact one of the Telephone numbers listed above.



### Translating and Interpreting Service (TIS)

TIS is an interpreting service provided by the Department of Home Affairs for people who do not speak English and for agencies and businesses that need to communicate with their non-English speaking clients.



TIS

13 14 50 (within Australia)

+613 9203 4027 (outside Australia)

TIS Online is available at: <http://tisnational.gov.au/>

## ANNEXURE - DETAILED PURPOSES FOR WHICH MPC COLLECTS, HOLDS, USES AND DISCLOSES PERSONAL INFORMATION

The purposes in more detail for which we collect, hold, use and disclose personal information are:

### ACT Cladding Program

MPC collects information on Private Properties and maintains a Register of Potential Suppliers as part of the ACT Cladding Program. Information collected under this program includes:

- Contact details of Strata Managing Agents and Executive Committee Members;
- Addresses and associated information of affected buildings;
- Contact names and contact details for affected buildings;
- Risk assessment information;
- Cost estimates of rectification work;
- Company and business details of potential suppliers, including contact details, Australian Business Numbers and Australian Corporation Numbers if applicable;
- Resumes of potential suppliers' key personnel;
- Corporate Capability Statements of potential suppliers;
- Insurance details of potential suppliers.

### Closed Circuit Television (CCTV)

MPC uses CCTV systems to monitor and record activity in a range of publicly accessible locations throughout the Directorate's worksites and office locations.

The purpose of this monitoring is to provide a safe and secure environment for staff and visitors. CCTV is used as a deterrence, investigation and emergency response management tool and for enforcement activities or incidents.

The information recorded and contained on corresponding files may include:

- identifiable images of people visiting the Directorate's locations;
- name and contact information;
- occupations, outcome of any review/investigation conducted; and
- details of witnesses to matters on CCTV recordings.

In accordance with the ACT Government Code of Practice for CCTV, signage is clearly displayed at all entry points and in prominent positions in waiting areas. Signage is also displayed in back-office areas where CCTV coverage occurs. The CCTV recorders are located within a secure area in each of the premises. Footage is only used or disclosed where there is a permitted exception under the TPPs.

## Community engagement

MPC manages a range of community engagement and stakeholder relations activities to inform policy, and program evaluation and development. We also conduct secretariat and nomination processes for certain boards.

We may collect, use and disclose personal information to facilitate:

- the functioning of various committees and boards;
- the organisation of events or ceremonies to present honours or awards, and
- addressing community engagement issues on particular matters.

## Corruption, Fraud and other investigations

The Executive Group Manager, Infrastructure Delivery Partners and Project Director, Light Rail are the Senior Executives Responsible for Business Integrity Risk (SERBIR). The SERBIR coordinates investigations into allegations of fraud and abuse of public office, that may also take the form of a Public Interest Disclosure (PID) in MPC.

We collect personal information in relation to personnel matters that arise through the provision of human resources advice and supporting workplace culture initiatives. We hold an individual file for each matter or investigation.

## Correspondence and communications

We hold personal information in branches across the Directorate to respond to requests for information from relevant business areas or our portfolio Ministers. This includes requests for Ministerial correspondence, requests for general correspondence or feedback.

If we receive a request from a third party, we will not disclose an individual's personal information without their consent and authority to do so, or where another permitted exception applies under the Information Privacy Act. This includes when responding to Ministerial correspondence or general feedback enquiries.

We use numerous communication channels to engage with the Canberra community and the public. For more information about these channels please refer to the section Whole-of-Government purposes for which we collect, use and disclosure personal information. Communications and engagement activities include: YourSay, the Community Relationship Management tool (CRM) and the YourSay Community Panel.

More information is also available in the section Submissions and surveys, and our Website Privacy Notice about how you may engage with us using social media platforms, for example, Facebook and Twitter.

## Financial and economic management

We collect and handle personal information to manage a range of financial activities including providing economic analysis and advice to ACT Government agencies, preparing the ACT Government's budget, expenditure review by ACT Government, and MPC's financial activities including accounts payable and receivable.

The kinds of personal information we collect, use, or disclose when providing financial and economic management functions or activities may include your:

- name and contact information;

- gender, occupation and salary information;
- personal opinions;
- financial details such as bank account details, credit card details, trading terms and conditions, establishing, operating and maintaining accounting systems, controls and procedures, financial planning, GST Declaration and other information associated with specific transactions; and
- claims against the ACT Government.

## Freedom of Information (FOI)

We collect personal information to administer the requirements for access to official documents under the *Freedom of Information Act 2016* (the FOI Act). Under s30 of the FOI Act, if making a request for personal information an applicant must provide evidence of identity. If an agent is acting for the applicant, they must provide evidence of their authorisation and of their own identity.

General freedom of information (FOI) records are secured by staff of Corporate Management, MPC. Access is limited to the FOI coordinator, relevant Managers and Executives, staff processing FOI requests, and Objective administrators. We may disclose personal information in these records for the purpose of conducting internal reviews and appeals to the ACT Ombudsman or the ACT Civil and Administrative Tribunal.

## Personnel information (ACTPS and contractors)

### General recruitment and ongoing employment

We collect and hold information about ACT Public Service (ACTPS) staff, including ongoing staff, non-ongoing staff, and contractors. We collect this information for the *primary purposes* of:

- recruitment and onboarding;
- probation and performance management or performance appraisals;
- appointments to Government Boards and Committees;
- the processing of salaries, payroll, and ICT services and assets;
- providing transport to staff, including ride sharing services, public transport, taxis, or bicycles;
- security clearances and security vetting;
- workplace health and safety;
- injury management (compensable and non-compensable injuries), rehabilitation and return to work activities;
- Public Interest Disclosure (PID);
- Code of Conduct investigations;
- managing government assets such as vehicles, PCs, laptops, government provided phones, entry and exit of buildings; and
- staff surveys.

Specific kinds of personal and sensitive information collected may include but are not limited to:

- tax file number;

- police checks;
- declaration of personal interests;
- declarations of conflicts of interest;
- declarations about second jobs;
- drivers licence details;
- Uber and MyWay Card (if registered) account details;
- training records;
- Australian Government Service (AGS) number;
- next of kin, emergency contacts or family information;
- information related to security clearance;
- staff development and training details;
- workstation assessment reports;
- medical or personal health information;
- compensation details;
- salary/payment details;
- salary packaging details, including reportable fringe benefit amounts, lease agreements, vehicle insurance details and vehicle registration numbers;
- superannuation fund details; and
- details of accounts with financial institutions.
- workplace behaviour

We may use or disclose personal information related to a Workplace Behaviour investigation to other staff within MPC, and/or to relevant third parties, including the complainant. Information related to a Workplace Behaviour investigation may also be disclosed to agencies which are authorised to receive information under their respective legislation, including law enforcement bodies where relevant.

### **Injury and Illness Management**

We may disclose the personal information of a staff member who has suffered a compensable illness or injury to persons within the ACT Government, including the staff member's case manager, the manager of their work area and relevant members of the Corporate Services HR team. Information can also be disclosed to third parties, including treating medical practitioners, independent specialists, any relevant third party or insurer considered to have contributed to the illness or injury, future employers and legal advisers.

## **Prequalification Schemes for Consultants**

MPC administers prequalification schemes for various suppliers. Information collected for this scheme includes;

- Company and business details of potential suppliers, including contact details, Australian Business Numbers and Australian Corporation Numbers if applicable;

- Insurance and Licence particulars;
- Staffing details and technical capacity including staff CV's;
- Referee contact details;
- Financial information.

## Procurement

To enable registration for prequalification and panels, and selection of contractors for the supply of goods, services and works, we may collect, use or disclose the personal information of individuals who are involved in procurement activities either as sole traders or as representative of their agency, organisation or business, for the provision of various products and services. This may include:

- name and contact information;
- occupation, employment history, qualifications, salary rates;
- gender, date of birth; and
- declarations of personal interest.

## Project Management And Reporting System (PMARS)

PMARS is an online tool which delivers a systematic approach to managing, reporting and delivering capital works projects for the ACT Government.

The PMARS Supplier Relationship Management (SRM) portal allows suppliers to lodge invoices and payment claims against current contracts you are party to. The SRM portal allows suppliers to view and manage a range of information including:

- Electronically submit payment claims and invoices;
- Track the payment status of invoices;
- Contract Securities (security type, receipt number, amount, date lodged and status);
- Communicate directly with Project Managers on specific contractual matters; and
- Update insurances and submit documentation.

## Public Interest Disclosure (PID)

The [Public Interest Disclosure Act 2002](#) governs the collection, use and disclosure of personal and sensitive information. Nominated Disclosure Officers, the Public Sector Standards Commissioner and the ACT Government Integrity Commissioner manage Public Interest Disclosures (PIDs).

Appointed staff in the Workforce Capability and Governance Division maintain an electronic tracking system register) for capturing, managing and reporting information relating to PIDs received and investigated across the ACT Public Sector.

## Quality assurance and internal audit

We hold personal information for the purpose of quality assurance and internal audit processes. This information is held by Corporate Management.

Internal Auditors are sourced from external companies and are required to sign a Deed of Confidentiality and conflict of interest statement that expresses how confidential information can be used and disclosed, prior to commencing the audit.

## Security passes

When security passes are issued, the information collected includes name, work location and identifying photos. The purpose of collecting personal information for the issuing of security passes is to assist with the:

- management of building security;
- WHS compliance,
- security incident reports;
- emergency management of buildings i.e. fire or evacuation; and
- to identify persons who enter the building.

Information about staff pass usage may be also used and disclosed in accordance with the *Workplace Privacy Act 2011* for the purposes of: the security of other workers and assets, audit and legal requirements, misconduct and underperformance, and to monitor the efficiency of government business processes and activities.

## Submissions and surveys

At times, we may consult with the community and seek written submissions or survey the public. In many cases you may make a submission or participate in a survey without having to identify yourself. If you do identify yourself, any submission you provide us, or survey results will generally be made publicly available. We make submissions and survey results publicly available for transparency and to encourage public debate.

If you do not want your identity to be made publicly available, you must advise us at the time you make your submission that you wish to remain anonymous, or that you want the submission to be confidential. All survey results or reports are de-identified, and your personal information will not be made publicly available.

MPC advises individuals not to include personal or sensitive information (their own or a third party's) in submissions or surveys, however, we may use that information to develop or improve policies and programs subject of the consultation. We reserve the right to not publish any submission or survey responses, in full or in part, particularly where a submission or survey response may contain personal or sensitive information of the individual making the submission or participating in the survey, or that of third parties.

