Privacy Policy

February 2025

Introduction

The Privacy Act 1988 (Privacy Act) requires entities bound by the Australian Privacy Principles (APPs) to have a privacy policy.

The High Speed Rail Authority (the Authority) is an APP entity and this privacy policy outlines the authority's personal information handling practices.

The Authority is committed to respecting your right to privacy and protecting your personal information in accordance with the Privacy Act and our policies and procedures.

This privacy policy will be reviewed and updated periodically to consider any new laws or technology, or when our information handling practices change. Updates will be published on our website (hsra.gov.au).

In this policy, **personal information** has the same meaning as defined in section 6 of the Privacy Act:

> *personal information means information or an opinion about an identified individual, or an individual who is reasonably identifiable:*
>
> *a. whether the information or opinion is true or not; and*
>
> *b. whether the information or opinion is recorded in a material form or not.*

Sensitive information is a subset of personal information with additional requirements under the Privacy Act and is defined as:

> *'information or an opinion about an individual's racial or ethnic origin, political opinions, membership of a political association, religious beliefs or affiliations, philosophical beliefs, membership of a professional or trade association, membership of a trade union, sexual orientation or practices, or criminal record that is also personal information; health information about an individual, genetic information about an individual, biometric information that is to be used for the purpose of automated biometric verification/identification and biometric templates'.*

What kinds of personal information are collected and held?

We collect personal information about you where it is reasonably necessary for, or directly related to, one or more of our functions or activities, including:

- Personnel records
- Work health and safety
- Contractor and consultancy details
- Mailing lists
- Freedom of Information requests
- Complaint and feedback information
- Contract, tender and submission documents
- Representations to the authority and minister and any written responses
- Correspondence initiated and related to the activities of the Authority

- Security clearance records
- Stakeholder and supplier

Sensitive information is afforded a high level of protection under the Privacy Act, including limited circumstances in which it can be collected.

The Authority does not normally have a need to collect the majority of the sensitive information referred to in the definition in the Privacy Act. The exception is information collected about you in relation to recruitment processes and employment with the Authority, including:

- criminal records
- health records (including information about your medical history and ongoing medical information) where relevant to assessing an application, making reasonable adjustments in a recruitment process or the management of your health and safety or the health and safety of all employees, or
- information relevant to a work health and safety assessment, incident or investigation.

Collection of information during recruitment

The HSRA completes recruitment through recruitment Agencies and via applications submitted directly by email in response to job advertisements on Seek. In order to apply for roles, Applicants submit personal details in their CV and further details are collected for police checks. Relevant personal information collected during recruitment includes the Applicant's names, date of birth, location of birth, citizenship, home address, email address, home telephone number and copies or images of identification documents.

Further personal information is collected from successful applicants via employee forms, superannuation forms and taxation forms.

The personal information of job applicants is collected and held to enable the management of recruitment processes as required by the *Public Services Act* 1999 and for the purposes of onboarding.

All positions within HSRA require a security clearance. HSRA's clearance process is required to comply with the requirements prescribed in the *Australian Government's Protective Security Policy Framework* and *Personnel Security Protocol*.

All information provided by Applicants for a security process is only used for assessing their suitability to hold the relevant security clearance.

Collection of information during stakeholder engagement

HSRA collects personal information about stakeholders during stakeholder engagement activities, such as through workshops, events, surveys, community information centres. Information can also be collected through correspondence such as emails and telephone calls and where people have contacted HSRA directly through social media. The personal information collected can include names, contact details (telephone number, email and in some cases address), organisation, general location, stakeholder group and details of the interaction.

Telephone calls to 1800 958 562 are handled by a third-party company, Well Done Call Centre, who collects information on behalf of HSRA and the information collected automatically feeds into a HSRA database. At community events, information can be collected via surveys completed directly by HSRA staff using an iPad. Workshops happen in a group setting that can involve roundtables. During workshops, there can be HSRA staff capturing communications and discussions that happen on roundtables.

The purpose of collecting the information during the stakeholder engagement activities is to enable HSRA to build awareness and support for the High-Speed Rail Network in Australia and update stakeholders about the

project. The information collected during stakeholder engagement is stored in a secure platform, Consultation Manager, which is accessible only by the Communications and Engagement team and is not disclosed externally by HSRA.

Stakeholders can also subscribe directly on the website to register for email updates. Personal information is collected during that process, including names and contact details (email address, suburb, post code and locations stakeholders are interested in). That information is collected for the purpose of communicating project updates to stakeholders.

Your choices

If you are listed on one or more of our stakeholder email lists or community engagement emails, you can opt out at any time by contacting HSRA directly. You can also unsubscribe by using the 'unsubscribe' options noted in our emails.

Collection of information via CCTV at the Newcastle Community Information Centre

HSRA operates 5 CCTV cameras at the HSRA Office in Newcastle Office, National High Speed Rail Hub, Community Information Centre (175 Scott Street, Newcastle) and can operate CCTV cameras at other HSRA office locations, as may be the case from time to time.

When entering HSRA Office locations, either as an employee of HSRA or member of the public, personal information in the form of personal images, can be captured by CCTV cameras.

HSRA collects and uses the personal information via CCTV predominately to enhance and ensure the safety and security of the staff and visitors at the HSRA offices and to prevent and respond to security incidents.

Notice of the collection is available via signage at the Community Information Centre and the collection notice on the HSRA website, which contains further information.

HSRA will disclose CCTV footage, as required by law. This may include the disclosure of personal information to law enforcement agencies.

Collection of information during procurement

Personal information (of contractors and consultants) is collected during procurement processes at HSRA. The personal information collected includes names, contact details, CVs, qualifications, bank account details (for vendor creation), signatures, referee reports and any personal interests within any declarations of conflict of interest.

HSRA uses AusTender, the Australian Government's central procurement information system, to publish Open Tenders. More limited tenders are sent to specific service providers via email. Service providers submit bids in response, and the personal information described above can be collected by HSRA as part of that process.

Commonwealth contracts have clauses that identify and provide processes to manage confidential information (including personal information) of both parties during the process.

Collection of information within declarations of conflicts of interest, gifts and benefits

Personal information of directors, employees, consultants and contractors of HSRA is collected during the declaring of conflicts of interest and the declaring of gifts, benefits and hospitality.

The personal information collected in declaration of gifts, benefits and hospitality can include names, signature, and their gifts and benefits declared, and details of the person or organisation who offered the gift, benefit or hospitality. The details of gifts and benefits to agency heads can be published, with some personal information such as names deidentified, on the Gifts and Benefits register on the HSRA website.

The collection assists with meeting the Australian Public Service values and guidance,[1] section 29 of the *Public Governance and Performance Act* 2013 (Cth) and is done in accordance with the HSRA policies, including the Gifts and Benefits Policy.

The personal information collected in declarations of conflict of interest, can include names, signatures and details of personal interests provided for the declaration, which can include real estate investments, shareholdings, trusts or nominee companies, company directorships or partnerships, other significant sources of income, significant liabilities, gifts, private business, employment, voluntary, social or personal relationships that could or could be seen to impact upon official responsibilities.

Declarations of conflict of interest can also include the personal details of immediate family members. HSRA will seek the specific consent of those family members to the collection.

The collection of personal information for the declarations of conflict of interest, supports HSRA and HSRA's employees and contractors compliance with the APS Values and Code of Conduct.

Collection of information on the HSRA website

The HSRA website has a privacy statement about the information collected when browsing, accessing and using the HSRA website at Privacy Statement | High Speed Rail Authority | High Speed Rail Authority.

How do we collect your personal information?

Where possible, we will collect your personal information directly from you or your authorised representative. In limited circumstances we may collect personal information about you from a third party (for example, another Australian Government department or a publicly available source). For example, if:

- it is not practicable to collect personal information from you
- you have consented to the personal information being collected from someone else, or
- the Authority is authorised or required by law to collect your personal information from someone else.

We also obtain personal information from third parties such as referees if you are seeking employment with the Authority. If we collect personal information about you, we will take reasonable steps to inform you of that collection including whether it will involve a third party, the reasons for collection and what usual uses and disclosures may occur. Where sensitive personal information is concerned, we will also seek your express consent for that collection unless a legal exception under the Privacy Act applies.

---

[1] See Guidance for Agency Heads - Gifts and Benefits | Australian Public Service Commission

How do we safeguard and store personal information?

We take all reasonable steps to protect the personal information we hold from misuse, interference and loss, and from unauthorised access, modification or disclosure.

Data security measures adopted by HSRA via the Department of Infrastructure to protect personal information, include:

- multifactor authentication for access to HSRA systems
- the use of strong and complex passwords,
- monitoring and logging technologies to detect and respond to privacy and security incidents
- the encryption of certain systems
- application controls on workstations
- robust access control measures

Your personal information will only be stored on a password protected ICT system which complies with the Australian Government Protective Security Policy Framework. This includes ensuring that information we store is only accessed by authorised officers that require access to undertake their official functions and roles and in order to safeguard the accuracy and completeness of information provided to us.

When information is no longer required, it is securely destroyed in accordance with the Archives Act 1983 and relevant disposal authorities or forwarded to National Archives.

If personal information that HSRA holds is lost, or subject to unauthorised access or disclosure, we will respond in line with the Officer of the Australian Information Commissioner's Data breach preparation and response – a guide to managing data breaches in accordance with the *Privacy Act* and the HSRA Notifiable Data Breach Response Plan.

How we use and disclose personal information

We only use and/or disclose information for the purposes for which it was collected (the primary purpose), unless an individual has consented to another use.

There are certain limited circumstances in which we may use or disclose information for a different purpose, known as a secondary purpose, where that purpose is:

- directly related to the primary purpose for which the information was collected
- required or authorised under an Australian law or has been ordered by a court or tribunal
- necessary to lessen or prevent a serious threat to the life, health or safety of any individual, or public health or safety
- a permitted general situation or health situation, as defined by the Privacy Act, or
- an enforcement related activity and the use or disclosure of the information is reasonably necessary.

If we use or disclose information for a purpose other than what it was originally collected for, we will keep a written notice of that use or disclosure as required by the APPs.

Disclosure of personal information overseas

We do not ordinarily disclose personal information overseas. Certain activities, including surveys may utilise services based overseas. The Privacy Collection Notice which accompanies each activity will identify these services.

Data Quality

We take steps to ensure that the personal information we collect is accurate, up to date and complete. These steps include maintaining and updating personal information when we are advised by individuals that their personal information has changed, and at other times as necessary.

How to access and seek correction of your personal information

You have a right to request access to personal information that we hold about you and to request its correction under the Privacy Act. Please note that we are not required to grant access in certain circumstances such as where access would have an unreasonable impact on the privacy of other individuals. If we refuse to grant you access to your personal information, we will provide you with reasons for that decision within 30 days, as well as the avenues available for you to complain about the refusal.

You may also request changes to your personal information if it is inaccurate, out of date, incomplete, irrelevant or misleading. There is no charge associated with making a request and we will process the request and provide access to the information within 30 days.

Before we disclose personal information to you, we will take reasonable steps to verify your identity. To access personal information, a written request should be sent to our Privacy Officer:

by email – privacy@hsra.gov.au

The *Freedom of Information Act* 1982 also provides the option to request access to documents held by the HSRA. Individuals can seek access to the personal information the HSRA holds about them and seek correction of that information by emailing their request to the FOI Coordinator at foi@hsra.gov.au.

Further information about freedom of information requests is available on the HSRA website.

Contacting us anonymously

For some interactions with us, you may be able to remain anonymous or use a pseudonym. If you contact us anonymously, we may require other kinds of non-identifying information to help us accurately understand or verify the subject of your enquiry.

Making a privacy complaint

You may submit a complaint about the way we have handled your personal information. Complaints should be in writing and sent to the Privacy Officer using the contact details above.

We will respond in writing within 30 days of receiving your complaint. If you are dissatisfied with the response you receive, you can contact the Office of the Australian Information Commissioner (OAIC). Further information about making privacy complaints through the OAIC can be found by visiting https://www.oaic.gov.au/privacy/privacy-complaints.

Data Breaches

HSRA has a Notifiable Data breach response plan that must be followed.

Employees and Suppliers (under the terms of their Contract for Services) are required to notify the Privacy Officer immediately should they become aware of the actual or suspected data breach by email at privacy@hsra.gov.au.

In the event of a data breach involving personal and sensitive information, is assessed to be an eligible data breach, HSRA is obliged to advise any individual where that breach is likely to result in serious harm.

The notification will include recommendations about the steps that should be taken by the impacted individuals in response to this breach. HSRA will also notify the OAIC of the eligible data breach.

Privacy Impact Assessments

The *Privacy (Australian Government Agencies – Governance) Australian Privacy Principles Code* 2017 (the Code) requires agencies, including HSRA, to conduct a Privacy Impact Assessment (PIA) for all high privacy risk projects and maintain a register of the Privacy Impact Assessments it conducts.

A privacy impact assessment is a systematic assessment of a project that identifies the impact that the project might have on the privacy of individuals, and sets out recommendations for managing, minimising and eliminating the impact.

PIAs completed by the HSRA since the Code commenced on 1 July 2018 are listed on the privacy impact assessment register on the HSRA website.

Staff members of HSRA should contact the Privacy Officer to determine if a Privacy Impact Assessment is required for any new project. The Privacy Officer can conduct a privacy threshold assessment to assess whether a Privacy Impact Assessment is required.

A project may be a high privacy risk project if it is considered that the project involves any new or changed ways of handling personal information that are likely to have a significant impact on the privacy of individuals.

The Privacy Officer may conduct a PIA internally at HSRA or seek for a PIA to be conducted externally via the Legal Service Panel or the Management Advisory Services (MAS) Panel, which is managed by the Department of Finance.

Further information about Privacy Impact Assessments at HSRA is within the Privacy Impact Assessment procedure and instruction document.

Privacy Management Plan

HSRA has a Privacy Management Plan (PMP) that identifies its specific, measurable privacy targets and goals. The PMP also explains how HSRA meets its obligations under APP 1.2.

The PMP measures the privacy maturity of HSRA. The PMP is a living document and is reviewed annually

Roles and Responsibilities

Privacy Officer

The Privacy Officer is the primary point of contact for advice on privacy matters and is responsible for:

- handling of internal and external privacy enquiries, privacy complaints, and requests for access to and correction of personal information.
- assisting with the preparation of privacy impact assessments (PIAs)
- maintaining HSRA's register of PIAS
- measuring and documenting HSRA's performance against is privacy management plan (PMP) at least annually.

Privacy Champion

The Privacy Champion is the GM Corporate Services and General Counsel who is responsible for:

- promoting a culture of privacy within HSRA that values and protects personal information
- providing leadership within HSRA on broader strategic privacy issues
- documenting review of HSRA's progress against the PMP
- providing regular reports to HSRA's executive, including about any privacy issues arising from HSRA handling of personal information.

Further information

For further information about how we manage personal information, see the privacy page of the HSRA website or contact the Privacy Officer using the above details. A summary of the Australian privacy principles that HSRA are required to follow are available in Schedule A.

For more general information on Privacy and Information access refer to the Office of the Australian Information Commissioner (OAIC) at www.oaic.gov.au or by telephone on 1300 363 992.

Schedule A – Australian Privacy Principles Quick Reference Guide

Principle	Title	Purpose
APP 1	Open and transparent management of personal information	Ensures that APP entities manage personal information in an open and transparent way. This includes having a clearly expressed and up to date APP privacy policy
APP 2	Anonymity and pseudonymity	Requires APP entities to give individuals the option of not identifying themselves, or of using a pseudonym. Limited exceptions apply.
APP 3	Collection of solicited	Outlines when an APP entity can collect personal information that is solicited. It applies higher standards to the collection of sensitive information

	personal information	
APP 4	Dealing with unsolicited personal information.	Outlines how APP entities must deal with unsolicited personal information.
APP 5	Notification of the collection of personal information	Outlines when and in what circumstances an APP entity that collects personal information must tell an individual about certain matters.
APP 6	Use or disclosure of personal information	Outlines the circumstances in which an APP entity may use or disclose personal information that it holds.
APP 7	Direct marketing	An organisation may only use or disclose personal information for direct marketing purposes if certain conditions are met.
APP 8	Cross-border disclosure of personal information.	Outlines the steps an APP entity must take to protect personal information before it is disclosed overseas.
APP 9	Adoptions, use or disclosure of government related identifiers	Outlines the limited circumstances when an organisation may adopt a government related identifier of an individual as its own identifier, or use or disclose a government related identifier of an individual.
APP 10	Quality of personal information	An APP entity must take reasonable steps to ensure the personal information it collects is accurate, up to date and complete. An entity must also take reasonable steps to ensure the personal information it uses or discloses is accurate, up to date, complete and relevant, having regard to the purpose of the use or disclosure
APP 11	Security of personal information	An APP entity must take reasonable steps to protect personal information it holds from misuse, interference and loss, and from unauthorised access, modification or disclosure. An entity has obligations to destroy or de-identify personal information in certain circumstances.
APP 12	Access to personal information	Outlines an APP entity's obligations when an individual requests to be given access to personal information held about them by the entity. This includes a requirement to provide access unless a specific exception applies.
APP 13	Correct of personal information	Outlines an APP entity's obligations in relation to correcting the personal information it holds about individuals.