INFORMATION PRIVACY POLICY

Owner	General Manager Corporate Services and Company Secretary
Author	Information and Privacy Manager
Content Manager Reference	D/25/9280
Approver	Executive Management Team
Effective Date	29 August 2025

Contents

1 Audience

This policy is for all South Bank Corporation (SBC) employees in relation to the personal information collected, stored, managed, used and disclosed in discharging the functions of SBC.

2 Purpose

The *Information Privacy Act 2009* (Qld) (IP Act) and its Queensland Privacy Principles (QPs) regulate how Queensland government agencies, including South Bank Corporation (SBC), handle personal information. These rules include a requirement, under QPs 1, that SBC has an Information Privacy Policy which explains:

- the kinds of personal information SBC collect and hold
- how SBC collect and hold that personal information
- the purposes for which SBC collect, hold, use and disclose personal information
- how to access or correct personal information
- how to complain about a breach of the QPs or Code and how SBC will deal with the complaint
- whether SBC are likely to disclose personal information outside Australia and to which locations
- how SBC deal with privacy breaches.

3 Responsibilities

ROLE	RESPONSIBILITIES
SBC Board	• Ensure governance oversight of privacy obligations under the IP Act. • Support transparent management of personal information in line with QPs. • Oversee SBC's compliance with privacy principles and legislative obligations.
Chief Executive Officer	• Ensure SBC meets its obligations under the IP Act. • Oversee privacy governance and accountability. • Promote compliance with privacy obligations across SBC. • Ensure appropriate privacy complaint handling and reporting.

ROLE	RESPONSIBILITIES
Executive Leadership Team	• Approve the Information Privacy Policy. • Promote compliance with privacy obligations across SBC. • Support implementation of privacy policies and procedures. • Champion privacy awareness and training initiatives.
Information and Privacy Team	• Conduct privacy training and awareness activities. • Review and update privacy procedures and the Information Privacy Policy. • Advise on privacy compliance and obligations under the IP Act. • Lead Privacy Impact Assessments for new systems or changes in data handling.
Senior Manager, Risk and Governance	• Support integration of privacy risk into broader governance and risk frameworks. • Ensure privacy is considered in business continuity and risk planning. • Provide strategic oversight of privacy compliance.
All Employees	• Complete mandatory privacy and security training. • Handle personal information in accordance with SBC's privacy obligations. • Respect principles of anonymity and pseudonymity where applicable Ensure personal information is accurate, secure, and used appropriately.

4 Obligations under the IP Act

The primary object of the IP Act is to provide for fair collection and handling of personal information in the public sector environment.

The IP Act:

- requires SBC to comply with the privacy principle requirements including the QPs
- regulates when personal information may be disclosed outside Australia
- outlines SBC's obligations regarding contracted service providers
- provides mechanisms for dealing with privacy complaints and data breaches
- provides for the Information Commission to undertake audits and to take enforcement action.

The QPs cover the following:

QPs 1	Open and transparent management of personal information
QPs 2	Anonymity and pseudonymity
QPs 3	Collecting solicited information
QPs 4	Dealing with unsolicited information
QPs 5	Notification of collection of personal information
QPs 6	Use and disclosure of personal information
QPs 10	Quality of personal information
QPs 11	Security of personal information
QPs 12	Access to personal information
QPs 13	Amendment of personal information.

Note: Queensland Privacy Principles 7, 8, and 9 do not apply to SBC as these principles are explicitly excluded from applying to Queensland Government agencies under the *Information Privacy Act 2009*

The IP Act also creates privacy obligations in relation to:

- Overseas transfer of personal information
- Contracted service providers
- Mandatory data breach notification.

5 Personal information

Personal information is:

> *information or an opinion about an identifiable individual or an individual who is reasonably identifiable, from the information or opinion –*
>
> *(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.*

Personal information includes a broad range of information that could identify an individual. What is personal information will vary depending on whether a person can be identified or is reasonably identifiable in the circumstances.

- An individual will be identified where they can be identified from the information itself, without referring to any other information.
- An individual may be reasonably identifiable if there is reasonable potential that multiple pieces of information could lead to their identity being known. The likelihood of an individual being reasonably identifiable will depend on multiple factors relevant to the information, the characteristics of the individual, and the agency's functions.

6 Corporation Information

SBC holds personal information when it is contained in a document in the possession, or under the control, of SBC. This may extend beyond physical possession of a document to include a document that SBC have the right to deal with. For example:

- where SBC physically possess a record containing the personal information and can access that information physically or by use of an electronic device (such as decryption software)
- where SBC have the right or power to deal with the personal information, even if the document is not in our physical possession or own the medium on which the personal information is stored.

7 Types of personal information

SBC collects personal information in relation to a range of functions and activities including for:

- Car parking
- Retail lease management
- Precinct maintenance and management
- Infrastructure planning and construction
- Liquor licensing
- Health and safety
- Incident management
- Community consultation and communication
- Events management
- Precinct security
- Marketing
- Commercial operations
- Contract management
- Corporate administration including financial, procurement and human resources.

The types of personal information SBC collects depends on the function or activity performed, but may include:

- Contact details including name, phone number, business, residential and email address
- Car registration
- Health and medical information
- Occupational and employment information including recruitment and selection information
- Criminal history

- Unique identifiers including tax file number, driver licence, birth certificate and passport details
- Images in CCTV and photographs
- Internet protocol and other IT information.

The IP Act has special rules around collecting sensitive information. Sensitive information is information or opinion about an individual:

- 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
- criminal record
- health information
- genetic information
- biometric information that is to be used for the purpose of automated biometric verification or biometric identification
- biometric templates.

SBC may collect sensitive personal information to perform its functions, including to:

- support recruitment and employment functions
- provide services to a person
- manage a complaint
- deal with precinct security or
- manage an incident relating to SBC or precinct management.

SBC only collects sensitive information directly from the individual and with their consent, or where SBC is otherwise authorised to collect the information.

8 Contracted service providers

The IP Act contemplates circumstances where public entities outsource services, functions or activities. Where SBC enters into a service arrangement for the provision of services that involves dealing with personal information, SBC must take all reasonable steps to bind the contracting service provider to the relevant parts of the IP Act, otherwise, the privacy obligations that would have attached to the contracted service provider in relation to that personal information, attach to SBC.

9 Disclosure outside of Australia

The IP Act recognises that there may be a risk to an individual's privacy if their personal information is disclosed to locations outside Australia, particularly if those locations do not have equivalent privacy protections.

SBC understands its obligations in relation to the disclosure our personal information out of Australia. Ordinarily, SBC will not disclose personal information overseas or engage service providers that store their records outside Australia without the agreement of the person, or where SBC is otherwise authorised.

SBC also takes steps to be satisfied that our service providers have appropriate controls to protect your personal information and that they only use personal information for purposes SBC authorises.

However, people should be aware that when they communicate with SBC through a social network service such as Facebook or Twitter or an email marketing platform, the provider and its partners may collect and hold the personal information overseas. In those cases, the privacy policies of those platforms regulate how the personal information is managed.

10 Anonymity & pseudonymity

There may be times when people will prefer to interact with SBC without using their real identity. In most cases, SBC will need a name and other personal information to properly deal with a matter or to provide a service. However, where practicable, people will have the option to interact with us anonymously or by using a pseudonym.

11 Collection of personal information

SBC collects personal information by various methods, including at face-to-face meetings, telephone calls, hard copy forms, web-based forms, emails, submissions, CCTV, photographs, web analytics, social media, subscription services, mailing lists and surveys.

Personal information must be collected by lawful and fair means so when SBC collects personal information directly from a person, steps are taken to make the person aware of the circumstances of the collection. Collection notices may be communicated in a variety of ways including:

- at the point of collection (website, form, or signage)
- through audio recording
- soon after collection (return acknowledgement email)
- referral to Privacy Collection Guide or Information Privacy Policy
- terms and conditions of entry to the South Bank precinct and carparks
- links to relevant information on precinct signage.

Occasionally, SBC will collect personal information from third parties, for example where:

- a representative has been authorised to deal with SBC on a person's behalf
- a visitor provides information about an incident in the precinct they have witnessed

- a referee provides a report on a person's capabilities.

Where practicable, SBC will ask the person for their consent before collecting their personal information from a third party.

12 Quality of personal information

SBC understands the importance of ensuring the personal information collected, used or disclosed is accurate, up-to-date and complete. The aim is to:

- accurately capture information in record-keeping systems
- confirm the accuracy of information collected from a third party where necessary
- take reasonable steps to check that personal information is accurate and current before using or disclosing it.

13 Use and disclosure of personal information

SBC uses and discloses personal information for the purpose it was collected unless one of the exceptions in QPs 6 (Use and Disclosure of Personal Information) apply.

SBC's functions and activities that require us to use or disclose personal information include for:

- events planning and hosting, and promoting activities in the precinct
- responding to or investigating an enquiry or incident
- security purposes and monitoring precinct activities
- conducting research for events planning and infrastructure development
- generating reports from data for business intelligence functions
- undertaking corporate administrative functions
- communicating about events and activities, issuing alerts about precinct infrastructure availability, disaster management and health and safety concerns.

SBC may also use or disclose personal information for secondary or alternative purposes as permitted under the IP Act, for example:

Statutory information sharing

SBC may disclose personal information where information sharing is authorised under relevant legislation, for example, to the Ombudsman, Privacy Commissioner, Human Rights Commissioner, Crime and Corruption Commission, Information Commissioner and Courts or Tribunals.

Complaints and reviews

If a complaint is made to SBC, it may be necessary for us to disclose information to the person alleged to be responsible and others for the purpose of properly assessing and investigating the complaint and to afford natural justice. SBC may also disclose personal information to a review or oversight body.

Data breach notifications

SBC is required to notify relevant bodies about information privacy breaches including the Queensland Information Commissioner for eligible data breaches and the Australian Information Commissioner in relation to Tax File Numbers. Refer to the SBC Data Breach Response Plan for further information.

Research, analysis or statistics

Consent is sought to use personal information for research, analysis or statistical purposes. However, if it is not practicable to obtain consent, and the research is in the public interest and does not involve publishing information that identifies individuals, then SBC may use or disclose the information. If the research process requires disclosing the personal information to another entity, SBC will take steps to ensure that they will not further disclose the information.

14 Storage and security

SBC holds personal information securely and takes reasonable steps to protect it from misuse, interference, loss, unauthorised access, modification or disclosure.

SBC comply with Queensland Government Information Standards and security protocols directed at ensuring that only authorised people can deal with personal information held by SBC.

Physical documents are held on site on secure floors or at secure offsite storage. Personal information held in electronic format is held on servers that are either on-premises or in tenancies in the cloud. SBC retains effective control over personal information held on cloud tenancies, and the information is managed in accordance with legislative obligations and relevant contractual terms and conditions.

SBC takes reasonable steps to protect the personal information it holds from internal and external threats. For example, SBC:

- apply mitigation strategies developed by the Australian Signals Directorate known as the 'Essential Eight,' including multi-factor authentication, restricted administrative privileges, regular back-ups, promptly implementing updates and patches
- implement audit and scanning controls to detect unauthorised access to SBC's systems and information (e.g. using another person's account; viewing, sharing or storing inappropriate material; and using unauthorised devices)
- keep a record of when personal information held in SBC's electronic systems is changed or deleted (subject to system capabilities)
- conduct periodical internal and external audits
- have information security policies and procedures, conduct awareness campaigns and provide mandatory staff training
- regularly review and update the Privacy Data Breach Response Plan to ensure that SBC meet obligations under the Mandatory Data Breach Notification Scheme
- undertake Privacy Impact Assessments when personal information handling practices change, or new systems are introduced.

15 Destruction or deletion of personal information

Personal information which is contained in an SBC record is subject to the requirements of the *Public Records Act 2023*, the General Retention and Disposal Schedule, and any other applicable Record Keeping Standards issued by the Queensland State Archivist.

If SBC does hold personal information that is no longer needed, and SBC is not required to retain it, SBC will take reasonable steps to destroy the information or to ensure the information is de-identified.

16 Access and correction

People have the right to ask for access to personal information that SBC holds about them. SBC facilitates access to certain types of personal information through administrative access arrangements, or where that is not appropriate, by formal application under the *Right to Information Act 2009* (RTI Act).

People also have a right to ask us to correct personal information SBC holds about them if they believe the information is inaccurate, out of date, incomplete, irrelevant or misleading. They may ask for it to be amended administratively, or where that is not appropriate, by formal application under the RTI Act.

17 Privacy Breaches

A privacy data breach is where there has been unauthorised access to or disclosure of personal information, or the loss of personal information.

If SBC becomes aware of an actual or suspected privacy data breach, immediate steps will be taken to:

- contain the breach and mitigate the harm
- assess whether affected persons should be notified and whether it is an eligible data breach requiring a notification to the Information Commissioner
- review what occurred and what action can be taken to prevent it happening again.

Refer to the SBC Data Breach Response plan for further information.

18 Privacy complaints

SBC has a privacy complaints process to deal with privacy complaints. A privacy complaint must be made in writing and in most circumstances, made within 12 months of the person becoming aware of the incident. Information about how to make a privacy complaint is available on our website.

In Queensland, the privacy complaint process consists of three tiers:

- South Bank Corporation: complaint made to SBC who has 45 business days to respond (or a further extension period).

- Information Commissioner: complaint made to the Information Commissioner if the response period has passed and a response has not been received, or if a response has been received, it is inadequate. The Information Commissioner has power to mediate the complaint.
- Queensland Civil and Administrative Tribunal (QCAT): if not satisfied with the outcome of the mediation, the complainant may ask the Information Commissioner to refer the complaint to QCAT for determination.

19 Relevant Legislation & Procedures

- *Information Privacy Act 2009 (Qld)*
- *Right to Information Act 2009 (Qld)*
- *Public Records Act 2002 (Qld)*

20 Contact

For further information, please contact: Information and Privacy Team
Email: privacy@south-bank.net.au

Version Updates

Version	Changes	Date
1.0	Initial document	29 August 2025