| Policy | **PIRSA** |
| --- | --- |

**IM P 011**

 PIRSA Information Privacy Policy IM P 011

SA Government and PIRSA information and ICT assets - including information received or held in business systems and databases (eg CHRIS, Masterpiece, Objective, PIIMS, SharePoint, TimeWise etc), email boxes, websites (eg PIRSA intranet, Internet website and social media sites), online applications, mobile phones, network/local drives, portable storage devices, cloud computing platforms (including Objective Connect, Skype for Business, Microsoft Teams, OneDrive for Business/Office 365, SharePoint Online); and office desks, filing cabinets, compactus and other physical storage or offsite/archive sites - and related processes will be managed in accordance with [SA Department of the Premier and Cabinet Circular PC012 - Information Privacy Principles Instruction](https://www.dpc.sa.gov.au/resources-and-publications/premier-and-cabinet-circulars/DPC-Circular-Information-Privacy-Principles-IPPS-Instruction.pdf), [SA Office for Data Analytics Standards and Guidelines](http://oda.sa.gov.au/content/data-sharing) and [SA Department of Premier and Cabinet Personal Information Data Breaches Guideline](https://digital.sa.gov.au/resources/personal-information-data-breaches) with respect to the collection, storage, access, correction, use, sharing and disclosure of personal information, and data breach response and notification requirements.

|  |
| --- |
| Document Control |
| **PPGS Owner Workgroup:** | Business Operations  | **PPGS Owner:** | Manager, Business Operations | **PPGS Risk Rating****& Review Cycle:** | High3 years  |
| **PPGS Contact Name:** | Lisa Farley | **PPGS Approver:** | Executive Director, Corporate Services | **Objective File & Document No.:** | CORP F2008/000124A5074270 |
| **PPGS Contact Title:** | Freedom of Information and Privacy Officer | **Date Approved:** | 29/06/2021 | **Status:** | Approved |
| **PPGS Contact Number:** | (08) 8429 0422 | **Next Review Date:** | 29/06/2024 | **Security Classification:** | 02 Official |

CONTENTS

[1. Purpose 4](#_Toc75788898)

[2. Scope 4](#_Toc75788899)

[3. Policy Details 5](#_Toc75788900)

[3.1 General Policy Principles 5](#_Toc75788901)

[3.2 Examples of Personal Information 7](#_Toc75788902)

[3.3 Ethics for handling information and making public comments 9](#_Toc75788903)

[3.4 Collection of personal information 10](#_Toc75788904)

[3.5 Storage and security of personal information 12](#_Toc75788905)

[3.6 Access and correction of personal information 14](#_Toc75788906)

[3.7 Use, sharing and disclosure of personal information 14](#_Toc75788907)

[3.8 Consent to use photographic images and video footage 17](#_Toc75788908)

[3.9 Contract clauses for service providers 18](#_Toc75788909)

[3.10 Protection of children, young people and their families 19](#_Toc75788910)

[3.11 Release of open data 20](#_Toc75788911)

[3.12 Cloud computing technologies 22](#_Toc75788912)

[3.13 Websites, online applications, mobile apps and social media sites 23](#_Toc75788913)

[3.14 Compliance reporting and exemptions 24](#_Toc75788914)

[3.15 Complaints 25](#_Toc75788915)

[3.16 Data Breach response and notification processes 25](#_Toc75788916)

[3.16.1 Data breach response processes 25](#_Toc75788917)

[3.16.2 Eligible data breach criteria 26](#_Toc75788918)

[3.16.3 Eligible data breach notification process 27](#_Toc75788919)

[3.16.4 Low risk data breach notification process 28](#_Toc75788920)

[3.16.5 Other data breach notification process considerations 28](#_Toc75788921)

[3.16.6 Information to be included in data breach notifications 30](#_Toc75788922)

[3.16.7 Reviewing existing data breach preventative measures and response processes 31](#_Toc75788923)

[4. Definitions 34](#_Toc75788924)

[5. Related Docum ents 39](#_Toc75788925)

| **REVISION RECORD** |
| --- |
| **Date** | **Version** | **Revision description** |
| 02/07/2015 | 0.1 | First draft of policy. |
| 08/10/2015 | 0.2 | Second draft of policy for internal review. |
| 17/03/2016 | 1.0 | Policy approved by the PIRSA Chief Executive. |
| 25/07/2013 | 1.1 | Minor updates to external hyperlinks. |
| 21/02/2018 | 1.2 | Minor updates to include new *Public Sector (Data Sharing) Act 2016*; and data breach response and notification processes in sections 6.7 and 6.16. |
| 25/03/2018 | 1.3 | Minor updates to include references to the new [*SA Department of Premier and Cabinet Personal Information Data Breaches Guideline*](https://digital.sa.gov.au/resources/personal-information-data-breaches)*.* |
| 29/06/2021 | 1.4 | Simplified text for Scope, converted into new template, inclusion of risk assessment, minor amendments including updates to external hyperlinks |
|  **RISK ASSESSMENT** |
| **Date** | **Risk Rating** | **Risk Assessment Evaluation** |
| 25/06/2021 | High | It is considered that not meeting the requirements of this policy and associated legislative, SA Government and PIRSA information security and privacy principles could have major consequences resulting in very serious harm to individuals, including physical, psychological, emotional, financial (including loss of business or employment opportunities) and reputational harm. A data breach could have a very serious impact on the reputation of PIRSA and the public’s trust in government agencies. |

# Purpose

The purpose of this policy is to provide clear policy principles on action that will be taken by PIRSA to ensure that:

* personal information collected or held will be securely stored; and only collected, transmitted, solicited, published, used, shared, disclosed and accessed in accordance with legislative, SA Government and PIRSA information security and privacy principles
* PIRSA employees, contractors, customers and service providers who have possession or control of SA Government and PIRSA information and ICT assets make appropriate amendments to those assets as are reasonable, to ensure that information assets are accurate, relevant, up-to-date, complete and not misleading
* The information subject (person to whom personal information relates) is entitled to have access to, and request reasonable amendments to information assets containing their personal information in accordance with the provisions of the [*Freedom of Information Act 1991*](http://www.legislation.sa.gov.au/LZ/C/A/FREEDOM%20OF%20INFORMATION%20ACT%201991.aspx)
* personal information data breaches are promptly assessed, investigated, reported and managed in accordance with legislative, SA Government and PIRSA data breach response and notification requirements outlined in this policy

# Scope

The policy applies to all SA Government and PIRSA information and ICT assets collected, stored, accessed, used, shared or disclosed by any means, including all physical or electronic data, documents, information, records, publications, websites, web pages, forms, images, sound, videos and related applications and technology.

The policy also applies to all providers and users of SA Government and PIRSA information and ICT assets, including employees, contractors, customers and service providers.

# Policy Details

## General Policy Principles

Whilst there is currently no State legislation regulating privacy in South Australia, PIRSA is subject to:

* the information privacy principles contained in the [SA Department of the Premier and Cabinet Circular PC012 - Information Privacy Principles Instruction](https://www.dpc.sa.gov.au/resources-and-publications/premier-and-cabinet-circulars/DPC-Circular-Information-Privacy-Principles-IPPS-Instruction.pdf);and supporting SA Government privacy guidelines and information sheets dealing with child protection, cloud computing, contracting and contract model clauses, open data, photographic images, and websites and online applications – which apply to the collection, storage, access, correction, use, disclosure and sharing of personal information collected or stored by PIRSA or shared with another agency.

The Privacy Committee of South Australia is responsible for overseeing the information privacy principles set out in [*DPC Circular PC012*](https://www.dpc.sa.gov.au/resources-and-publications/premier-and-cabinet-circulars/DPC-Circular-Information-Privacy-Principles-IPPS-Instruction.pdf)and providing advice on privacy issues

* personal information data breach response and notification requirements described in the [*SA Department of Premier and Cabinet Personal Information Data Breaches Guideline*](https://digital.sa.gov.au/resources/personal-information-data-breaches)
* the relevant provisions of the [*Privacy Act 1988*](https://www.legislation.gov.au/Series/C2004A03712) (Commonwealth), which governs the collection, use, storage and disclosure of personal information about individuals in the custody of the Australian Government; and the individual’s right to access their personal information held by Australian Government agencies and have it corrected if it is incorrect.

The [Privacy Act](https://www.legislation.gov.au/Series/C2004A03712) also legislates the application of the [*Australian Privacy Principles*](https://www.legislation.gov.au/Series/C2004A03712) (published as Schedule 1 of the [Privacy Act](https://www.legislation.gov.au/Series/C2004A03712)) to Australian Government agencies; major Australian business and not-for-profit organisations; service providers contracted by the Australian Government; and some smaller business operators such as private sector health service providers, businesses that sell or purchase personal information, employee associations, consumer credit providers and reporting bodies (including utilities and telecommunications providers) and other organisations/providers.

State Governments, including SA Government agencies, are **not** generally subject to the [Privacy Act](https://www.legislation.gov.au/Series/C2004A03712) (Commonwealth) except in relation to:

* SA Government agencies receiving or dealing with Australian Government information for sharing, transfer, regulating or other purposes
* private sector organisation practices in disclosing information to State Governments
* the collection, storage, use, disclosure, security and disposal of tax file number (TFN) information in accordance with *[Privacy (Tax File Number) Rule 2015](https://www.legislation.gov.au/Details/F2015L00249/Explanatory%20Statement/Text)* issued under section 17 of the [Privacy Act](https://www.legislation.gov.au/Series/C2004A03712)
* data breach response and notification requirements mandated under the [*Australian Government Notifiable Data Breaches Scheme*](https://www.oaic.gov.au/privacy-law/privacy-act/notifiable-data-breaches-scheme) (established in accordance with the [*Privacy Amendment (Notifiable Data Breaches) Act 2017*](https://www.legislation.gov.au/Details/C2017A00012)) for eligible data breaches involving TFN information held by SA Government agencies, where such breaches are likely to cause serious harm to individuals.

**Note**: other jurisdictions also have privacy legislation (eg the [*Victorian Privacy and Data Protection Act 2014*](http://www.austlii.edu.au/au/legis/vic/num_act/padpa201460o2014317/)), which must be considered when SA Government agencies share, transfer or deal with personal information across federal and other state jurisdictions

* SA Government and internal agency information security risk and classification requirements, including those prescribed in the:
* [*SA Government Information Security Management Framework*](http://digital.sa.gov.au/resources/topic/policies-guidelines-and-standards/security/information-security-management-framework)and[*SA Office for Data Analytics Standards and Guidelines*](http://oda.sa.gov.au/content/data-sharing)
* [*PIRSA Protective Security Policy PR P 005*](https://objectivesag.pirsa.sa.gov.au/id%3AA307359/document/versions/published), [*PIRSA Information and ICT Security Policies, Procedures and Guidelines*](http://intranet.pirsa.sa.gov.au/documents/policies_and_procedures/ict_helpdesk/security_and_policies), [*PIRSA Document and Records Management Policy IM P 002*](https://objectivesag.pirsa.sa.gov.au/id%3AA49559/document/versions/published)and [*PIRSA Document and Records Management Access Controls and Security Guideline IM G 007*](https://objectivesag.pirsa.sa.gov.au/id%3AA2544/document/versions/published) (**Note:** these PIRSA links are only accessible to SA Public Sector employees on the SA Government StateNet or PIRSA IT Networks).

**In recognition of the importance of information privacy, all PIRSA employees, contractors and service providers are responsible for:**

* **maintaining the security and confidentiality of information and ICT assets collected, transmitted, solicited, published, used and accessed and/or for which they are the custodian**
* **keeping appropriate records relating to the provision of access to these assets.**

The principles outlined in this policy draw significantly from the:

* [*DPC Circular PC012*](https://www.dpc.sa.gov.au/resources-and-publications/premier-and-cabinet-circulars/DPC-Circular-Information-Privacy-Principles-IPPS-Instruction.pdf)*,* [*SA Government Privacy Guidelines for SA Government Websites and Online Applications*](https://archives.sa.gov.au/managing-information/releasing-information-and-privacy/privacy-south-australia/privacy-guidelines-and-information-sheets)and other supporting SA Government privacy guidelines and information sheets
* [*SA Government Information Security Management Framework*](http://digital.sa.gov.au/resources/topic/policies-guidelines-and-standards/security/information-security-management-framework),
* [*SA Office for Data Analytics Standards and Guidelines*](http://oda.sa.gov.au/content/data-sharing),

and other legislative, SA Government and PIRSA requirements.

## Examples of Personal Information

Personal information is defined as information or an opinion, whether true or not, relating to a natural person or the affairs of a natural person whose identity is apparent, or can be reasonably ascertained, from the information or opinion.

This includes combinations of name, address, date of birth, financial or health details or status, ethnicity, gender, religion, witness statements, alleged behaviours, licensing details, photographs or video footage of individual information subjects.

Examples of personal information about customers, employees and the general public that PIRSA may collect, transmit, solicit, store, publish, access, use and/or hold in paper form, verbally or through electronic means include information assets:

* created, stored, accessed, published and processed in business systems, databases and online applications (‘apps’) (eg CHRIS, Masterpiece, Objective, PIIMS, SharePoint, TimeWise, etc), personal computers, email boxes, network/local drives, websites (including the PIRSA intranet, Internet website and social media sites), cloud computing platforms (including Objective Connect, Microsoft Skype for Business, Microsoft Teams, OneDrive for Business/Office 365, SharePoint Online), portable storage devices (including USBs, laptops/notebooks/netbooks), external hard drives, iPads and Windows tablets, personal digital assistants (such as Pocket PC, Palm and Blackberry), CDs, DVDs, flash cards, CF cards, SD cards and other devices with in-built accessible storage (such as digital cameras, iPods, iPhones and other smartphones), and mobile devices
* in hard copy or paperformat such as applications, briefings, contracts, forms, hand-written notes, leases, legal documents, letters, licences, ministerial correspondence, minutes and memos, opinions, plans, presentations, reports, research, sticky notes, technical records, telephone messages/records, etc., including documents or other information stored in office desks, filing cabinets, compactus and other physical storage or offsite/archive sites
* in electronic format such as emails, e-business transactions, social media records, digital images, spreadsheets, websites, online applications, databases, word processing documents and other electronic documents or data. This includes internal and external user and client information and email addresses collected or stored in computer logs via websites, online forms, e-business transactions, business systems, mobile devices, social media tools, online applications, cloud computing platforms and system audit trails
* relating to primary industry sector and regions stakeholders, including those involved in agriculture, aquaculture, corporate, fisheries, food, forestry, wine, biosecurity, emergency management, rural services and scientific research sectors. This also includes industry board and committee members
* relating to customers, financial grant and sponsorship applicants, including sensitive financial, credit card, TFNs, electronic funds transfer and other banking information
* relating to recipients of fines and penalties of those who commit an offence or are prosecuted in relation to regulation of primary industries
* in the form of mailing lists such as those used for marketing and publication distribution purposes
* relating to contractors, consultants and service providers engaged by PIRSA to perform services, including contract agreement details such as contractor/contractor names, organisational details, Australian Business Numbers (ABN), consulting fees/rates and insurance arrangements
* relating to employees, particularly in relation to recruitment and selection, employment contracts and conditions, remuneration and other payroll information, emergency contact details, known medical conditions, employee/contractor TFNs, ICT assets and mobile and portable storage devices, motor vehicles, performance development and management, allowances and reimbursements, security, travel (including travel advance and travel expense reimbursement electronic funds transfer and other banking details), work health safety, injury management and other claims
* in the form of photographic images or video footage of customers, employees or members of the public used in PIRSA publications such as annual reports, banners, brochures, digital communications, factsheets, newsletters, podcasts, posters, presentations, social media sites, strategic plans, videos, websites and information sheets.

## Ethics for handling information and making public comments

PIRSA employees and contractors are subject to the ‘handling official information’ and ‘public comment’ provisions of the [*Code of Ethics for the South Australian Public Sector*](http://publicsector.sa.gov.au/policies-standards/code-of-ethics/)*,* which require SA Public Sector employees to:

* not access or attempt to access SA Government or PIRSA information other than in connection with the performance by them of their duties and/or as authorised
* not disclose information acquired through the course of their employment other than is required by law or where appropriately authorised in the agency concerned
* not misuse information gained in their official capacity, including, but not limited to, seeking to use information for personal benefit or gain or for the personal benefit or gain of another
* maintain the integrity and security of information for which they are responsible
* only make public comment in relation to their duties, the SA Public Sector or the SA Government when specifically authorised to do so. Public comment includes providing information or comment to or in any media (electronic and print), including comments posted on the Internet and made during speaking engagements
* ensure the privacy of individuals is maintained and will only release information in accordance with relevant legislation, industrial instruments, policy, or lawful and reasonable direction.

Other legislative, SA Government and PIRSA requirements for handling information and making public comments, including those outlined in this policy, also exist.

## Collection of personal information

[*DPC Circular PC012*](https://www.dpc.sa.gov.au/resources-and-publications/premier-and-cabinet-circulars/DPC-Circular-Information-Privacy-Principles-IPPS-Instruction.pdf)requires PIRSA to ensure that:

* personal information is not collected by unlawful or unfair means, or collected unnecessarily
* the information subject (person to whom the information relates) is informed of:
* the purpose for which the information is being collected
* if the information is authorised or required to be collected by law, that this is the case
* the usual practices with respect to the disclosure of personal information of the kind being collected
* personal information that is inaccurate, irrelevant, out of date, incomplete or excessively personal is not to be collected.

The [*SA Government Privacy Guidelines for SA Government Websites and Online Applications*](https://archives.sa.gov.au/managing-information/releasing-information-and-privacy/privacy-south-australia/privacy-guidelines-and-information-sheets)require PIRSA websites, online applications (‘apps’) and online forms that collect personal information to:

* comply with the above information privacy principles requirements
* not collect or solicit any personal information via websites or online ‘apps’ that would be unnecessary or unreasonably intrusive, inaccurate, irrelevant, out of date, incomplete, excessively personal, unlawful, unfair or unrelated to its function
* prominently display a message or link to a privacy statement on its websites, online ‘apps’ and online forms which state what information is collected about individuals and for what purpose; the legal authority for the collection if it is authorised by law; how this information is to be used; if it is to be disclosed and to whom; the risks to the individual of using the Internet as the transmission medium; other options for providing information; and any security tools and measures such as encryption products and level of protection to be used.

Examples of privacy statements for agency websites, online ‘apps’ and online forms are provided in the [*SA Government Privacy Guidelines for SA Government Websites and Online Applications*](https://archives.sa.gov.au/managing-information/releasing-information-and-privacy/privacy-south-australia/privacy-guidelines-and-information-sheets).

The above guidelines also discuss the collection and logging of information by website hosts about individuals visiting a website which will not in itself identify an individual. This includes clickstream data and cookies – either of which may not capture personal information as defined in the information privacy principles. However, it is recommended that in the interests of transparency, PIRSA Internet website, online application, mobile app and social media site privacy statements specify what clickstream data is collected; and how any cookies are used and for what purpose (refer section 3.13).

## Storage and security of personal information

[*DPC Circular PC012*](https://www.dpc.sa.gov.au/resources-and-publications/premier-and-cabinet-circulars/DPC-Circular-Information-Privacy-Principles-IPPS-Instruction.pdf)and[*PIRSA Protective Security Policy PR P 005*](https://objectivesag.pirsa.sa.gov.au/id%3AA307359/document/versions/published) (Note: this PIRSA link is only accessible to SA Public Sector employees on the SA Government StateNet or PIRSA IT networks) require PIRSA to ensure that:

* employees take steps to make certain that confidential, sensitive or personal information is not misused; and is securely stored when employees are in the office, absent from the workplace, travelling or in-transit in accordance with the information’s security classification.

Where appropriate, this may include secure transmission of electronic information; and storage of physical information in a safe, locked filing cabinet or compactus to prevent such information sitting on desks left unattended or in offices, venues or accommodation facilities that are unsupervised

* where highly sensitive, confidential or personal information is received, created, stored or discussed, physical access to offices, rooms, facilities and other areas is restricted
* if it is necessary for information assets containing personal information to be given to another person in connection with the provision of a service, everything reasonable is done to prevent the unauthorised use, disclosure or sharing of information contained within the information assets.

Refer to the [*PIRSA Protective Security Policy PR P 005*](https://objectivesag.pirsa.sa.gov.au/id%3AA307359/document/versions/published) for further information (Note: this PIRSA link is only accessible to SA Public Sector employees on the SA Government StateNet or PIRSA IT Networks).

The [*SA Government Privacy Guidelines for SA Government Websites and Online Applications*](https://archives.sa.gov.au/managing-information/releasing-information-and-privacy/privacy-south-australia/privacy-guidelines-and-information-sheets)require PIRSA to ensure that:

* personal information collected via its websites is done via sufficiently secure means
* individuals are advised of any other options for providing personal information, and what security tools and measures such as encryption products are in place
* internal networks, online ‘apps’, online forms, business systems and databases which contain personal information are sufficiently protected from unauthorised access via their websites and any Internet connections using firewalls or other technologies.

The [*PIRSA Document and Records Management Policy IM P 002*](https://objectivesag.pirsa.sa.gov.au/id%3AA49559/document/versions/published)and associated [*PIRSA Document and Records Management Access Controls and Security Guideline IM G 007*](https://objectivesag.pirsa.sa.gov.au/id%3AA2544/document/versions/published)(Note: these PIRSA links are only accessible to SA Public Sector employees on the SA Government StateNet or PIRSA IT Networks) alsorequire access controls and security protocols to be identified and applied to documents and records at the time of creation, receipt and capture. This is to ensure that these information assets - and any related confidential, private, sensitive or intellectual property information - are protected from inappropriate access, usage, disclosure, sharing or alternation; and comply with legally enforceable rights of access to information embodied in legislation.

Furthermore, the [*SA Government Information Security Management Framework*](http://digital.sa.gov.au/resources/topic/policies-guidelines-and-standards/security/information-security-management-framework) requires agencies to:

* as part of an information and data management plan, define authorised access for all its information assets, including who has access, the level of authority required and the level of access allowed in accordance with the policies, standards and controls for the protection of information in SA Government ICT environments described in the [*SA Government Information Security Management Framework*](http://digital.sa.gov.au/resources/topic/policies-guidelines-and-standards/security/information-security-management-framework)
* ensure information security management control measures are implemented for ICT assets to provide adequate protection over those assets in line with [*DPC Circular PC012*](https://www.dpc.sa.gov.au/resources-and-publications/premier-and-cabinet-circulars/DPC-Circular-Information-Privacy-Principles-IPPS-Instruction.pdf).

Information custodians must ensure that:

* information assets held, used or controlled by them containing personal information are protected and stored correctly in line with the [*PIRSA Protective Security Policy PR P 005*](https://objectivesag.pirsa.sa.gov.au/id%3AA307359/document/versions/published) (Note: this PIRSA link is only accessible to SA Public Sector employees on the SA Government StateNet or PIRSA IT Networks)
* personal information is checked for accuracy before it is collected, transmitted, solicited, published, used, shared or disclosed in accordance with this policy.

## Access and correction of personal information

[*DPC Circular PC012*](https://www.dpc.sa.gov.au/resources-and-publications/premier-and-cabinet-circulars/DPC-Circular-Information-Privacy-Principles-IPPS-Instruction.pdf)requires PIRSA to ensure that:

* The information subject (person to whom the information relates) of information assets containing personal information held or controlled by PIRSA is legally entitled to have access to such information in accordance with section 12 ‘Right of access to agencies’ documents’ of the [FOI Act](http://www.legislation.sa.gov.au/LZ/C/A/FREEDOM%20OF%20INFORMATION%20ACT%201991.aspx)
* if the information subject is aggrieved by the information assets held by PIRSA, they may apply for an amendment of the information in accordance with ‘Part 4 – Amendment of Records’ of the [FOI Act](http://www.legislation.sa.gov.au/LZ/C/A/FREEDOM%20OF%20INFORMATION%20ACT%201991.aspx)
* PIRSA employees, contractors and service providers who have possession or control of information assets that contain personal information will make appropriate corrections, deletions and additions as are, in the circumstances, reasonable to ensure that the information is accurate, relevant, up-to-date, complete and not misleading.

The [*SA Government Privacy Guidelines for SA Government Websites and Online Applications*](https://archives.sa.gov.au/managing-information/releasing-information-and-privacy/privacy-south-australia/privacy-guidelines-and-information-sheets) require PIRSA website, online ‘app’ and online form privacy statements to provide details on how customers, employees and members of the public can apply for access to their own information in accordance with the [FOI Act](http://www.legislation.sa.gov.au/LZ/C/A/FREEDOM%20OF%20INFORMATION%20ACT%201991.aspx), including legal rights to apply to correct personal information that is out of date, incorrect or misleading (refer section 3.13).

## Use, sharing and disclosure of personal information

[*DPC Circular PC012*](https://www.dpc.sa.gov.au/resources-and-publications/premier-and-cabinet-circulars/DPC-Circular-Information-Privacy-Principles-IPPS-Instruction.pdf)requires PIRSA to ensure that personal information in information assets held or controlled by PIRSA will not be used except for a purpose to which the information was disclosed, unless the:

* Information subject (person to whom the information relates) has given express or implied consent to disclose that information
* use, disclosure or sharing of personal information is:
* necessary for the health or protection of human life
* required by law
* reasonably necessary for the enforcement of the criminal law, a law imposing a pecuniary penalty, for the protection of the public revenue or for the protection of the interests of the SA Government.

The [*SA Government Privacy Guidelines for SA Government Websites and Online Applications*](https://archives.sa.gov.au/managing-information/releasing-information-and-privacy/privacy-south-australia/privacy-guidelines-and-information-sheets) require PIRSA to only publish personal information regarding individuals on the web if:

* it complies with the above information privacy principles
* the information subject (person to whom the information relates) is made aware of the risks associated with disclosure, including information being able to be searched by, made accessible to and copied by millions of web users from across the world; and has given informed consent

(refer section 3.13).

When developing information sharing arrangements with Australian/federal, state/territory and local government public sector organisations, including other SA Government agencies, consideration must be given to:

* legislative requirements issued under the [*Public Sector (Data Sharing) Act 2016*](https://www.legislation.sa.gov.au/LZ/C/A/PUBLIC%20SECTOR%20%28DATA%20SHARING%29%20ACT%202016.aspx) and associated [*SA Office for Data Analytics Standards*](http://oda.sa.gov.au/content/data-sharing)relating to trusted access principles and data sharing safeguards for the safe and secure sharing and use of public sector data with other departments. These include:
	+ requirements relating to data capture, classification, metadata, transfer, publishing analysis, annual reporting, security and use of identified/personal information
	+ requirements to complete [*SA Office for Data Analytics Data Sharing Request and Approval Forms*](http://oda.sa.gov.au/content/data-sharing)forreview, assessment and approval by the SA Government Chief Data Officers Network prior to sharing public sector data
	+ legislative protections for the authorised release of information between government departments
	+ restrictions on further use and disclosure of public sector data once shared
* data sharing risks, public value, governance, access, privacy, confidentiality, cultural, intellectual property, security and other considerations.

PIRSA employees, contractors, consultants and service providers may inadvertently neglect information privacy principles by distributing PIRSA reports or other information assets to external persons or organisations; or publishing personal information on the Internet, social media sites and in ‘apps’, including documents or other objects containing private information such as employee telephone lists containing work contact information, employee salary classification levels and other personal details. They may overlook the fact that these information assets may contain personal information collected by PIRSA for their formation.

Therefore, the PIRSA information custodian responsible for holding or controlling any information assets containing personal information must:

* check the accuracy of that information before it is used or disclosed
* ensure any unnecessary personal information is removed from information assets to be distributed to external organisations or persons; or published on the Internet, ‘apps’ and social media sites. This is to avoid employee exposure to unsolicited email/spam; unwelcome attention from a range of people and organisations; employees being harassed or their safety being adversely comprised; and other risks.

The PIRSA Freedom of Information and Privacy Officer (email PIRSA.FOI@sa.gov.au or phone (08) 8429 0422) can be consulted to seek advice regarding requests for the release of information which are not covered by the normal operational procedures, legislative requirements or the procedures stated in the [FOI Act](http://www.legislation.sa.gov.au/lz/c/a/freedom%20of%20information%20act%201991.aspx)*.*

When the requirement for the disclosure, sharing or use of personal information applies, it must be documented and adhered to between PIRSA and the organisation/person requesting the information.

**All decisions to release personal information to external parties** (eg auditors, actuaries, service providers, etc) **engaged by PIRSA for specific purposes must be consented to/approved, documented and controlled by the information subject** (person to whom the information relates);unless otherwise permitted and appropriately authorised under the provisions of the [Public Sector (Data Sharing) Act](https://www.legislation.sa.gov.au/LZ/C/A/PUBLIC%20SECTOR%20%28DATA%20SHARING%29%20ACT%202016.aspx) and associated [*SA Office for Data Analytics Standards*](http://oda.sa.gov.au/content/data-sharing).

## Consent to use photographic images and video footage

The [*SA Government Photographic Images and Privacy Information Sheet*](https://archives.sa.gov.au/sites/default/files/documentstore/policies-guidelines/Advice%20Sheet/photographic_images_and_privacy_-_information_sheet.pdf) identifies that photographic images or video footage for promotional purposes constitutes personal information as defined in [*DPC Circular PC012*](https://www.dpc.sa.gov.au/resources-and-publications/premier-and-cabinet-circulars/DPC-Circular-Information-Privacy-Principles-IPPS-Instruction.pdf).

PIRSA often uses images of people for promotional purposes. This can include photographic images or video footage of customers, employees or members of the public used in publications such as annual reports, banners, brochures, factsheets, newsletters, podcasts, posters, presentations, strategic plans, videos, websites and information sheets. When using photographic images or video footage, the Privacy Committee of SA encourages agencies to show regard to an individual’s right to exercise control over the use of their image. Therefore, PIRSA should obtain informed consent from the individual. In circumstances where it is difficult to gain informed consent such as a large event, PIRSA should consider giving notice to people attending the function that photographs or video footage will be taken and used for specific purposes.

While some organisations (eg the media) are exempt from the provisions of the [Privacy Act](https://www.legislation.gov.au/Series/C2004A03712), SA Government agencies are still subject to the disclosure provisions of the information privacy principles. **Consent should always be sought when considering the disclosure or sharing of photographs or video footage of individuals to external organisations**.

PIRSA photography and video consent forms for adults and children are available from the PIRSA intranet [Media, Communications, Marketing and Engagement](http://intranet.pirsa.sa.gov.au/documents/forms_and_templates/media_communications_marketing_publishing) site (Note: this PIRSA link is only accessible to SA Public Sector employees on the SA Government StateNet or PIRSA IT Networks).

## Contract clauses for service providers

[*DPC Circular PC012*](https://www.dpc.sa.gov.au/resources-and-publications/premier-and-cabinet-circulars/DPC-Circular-Information-Privacy-Principles-IPPS-Instruction.pdf)*:*

* allows SA Government agencies to disclose personal information to contracted service providers to provide services on behalf of the SA Government without breaching the information privacy principles
* stipulates that an agency contract for service provision which will necessitate the disclosure of personal information to a contracted service provider must include conditions to ensure that the information privacy principles are complied with as if the contracted service provider were part of the agency. A contract for service should also include provisions to enable audit and verification of compliance with these obligations. This is intended to ensure that the service provider’s responsibility for the collection, storage, security, access, use, disclosure, sharing and ownership of the information is beyond doubt.

The [*SA Government Contracting and the Information Privacy Principles Information Sheet*](https://archives.sa.gov.au/managing-information/releasing-information-and-privacy/privacy-south-australia/privacy-guidelines-and-information-sheets) requires agency contracts that involve the handling of personal information to include the obligations on the service provider to ensure personal information is managed in line with [*DPC Circular PC012*](https://www.dpc.sa.gov.au/resources-and-publications/premier-and-cabinet-circulars/DPC-Circular-Information-Privacy-Principles-IPPS-Instruction.pdf).

A set of [*SA Government Model Terms and Conditions Clauses for the Information Privacy Principles and Records Management*](https://archives.sa.gov.au/sites/default/files/documentstore/policies-guidelines/Guideline/model_terms_and_conditions_-_ipps_and_records_management.pdf) have been developed by the Crown Solicitor’s Office to assist agencies to meet information privacy principles and records management obligations prescribed in the [*SA Government Contracting and Official Records Standard*](https://archives.sa.gov.au/node/5998)*.*

Where relevant, consideration should also be given to including contract clauses relating to:

* legislative provisions under the [Public Sector (Data Sharing) Act](https://www.legislation.sa.gov.au/LZ/C/A/PUBLIC%20SECTOR%20%28DATA%20SHARING%29%20ACT%202016.aspx); and associated [*SA Office for Data Analytics Standards*](http://oda.sa.gov.au/content/data-sharing)relating to trusted access principles and data sharing safeguards, for the safe and secure sharing and use of public sector data with other departments, where a service provider or other third party is specifically authorised to share such data on PIRSA’s behalf (refer section 3.7)
* personal information data breach assessment, investigation, reporting, management and notification requirements if a service provider or other third party processes personal information, including tax file number (TFN) information, on PIRSA’s behalf (refer section 6.16).

## Protection of children, young people and their families

The *[SA Government Information Privacy Principles and Child Protection Information Sheet](https://archives.sa.gov.au/managing-information/releasing-information-and-privacy/privacy-south-australia/privacy-guidelines-and-information-sheets)* highlights that the information privacy principles are intended to work with the [*Children’s Protection Act 1993*](http://www.legislation.sa.gov.au/lz/c/a/childrens%20protection%20act%201993.aspx)and otherlaws and policies to promote the protection of children and young people; and should not represent a barrier to the collection, use, sharing or disclosure of information necessary to promote the protection of children and young people. The information privacy principles recognise that privacy is not an absolute right, and must be balanced against other important rights and interests. This includes the right of children and young people to be protected from harm.

The [*SA Government Information Sharing Guidelines for Promoting Safety and Wellbeing*](https://www.dpc.sa.gov.au/__data/assets/pdf_file/0009/45396/Information-Sharing-Guidelines.pdf) are designed to give providers of services to children, young people and adults confidence in sharing information where there are threats to safety and wellbeing where there is reasonable suspicion that individuals or groups are at risk of harm; and it is believed information sharing can support effective service intervention.

These guidelines provide a practical framework and step-by-step process for secure, timely, accurate and relevant recordkeeping, information sharing and disclosure practices. They also require informed consent for the disclosure of information to be sought from the information subject wherever safe and possible. When it is unsafe or impossible to seek consent and the person disclosing the information believes, on reasonable grounds, that the disclosure is necessary to prevent or lessen a serious threat to the life, health or safety of a person, personal information may be disclosed.

Business divisions need to consider how they manage information relating to children, young people and their families from the point of collection through to disposal; including ensuring that information and ICT assets are subject to appropriate security classification of information as outlined in the [*SA Government Information Security Management Framework*](http://digital.sa.gov.au/resources/topic/policies-guidelines-and-standards/security/information-security-management-framework)*,* [*PIRSA Protective Security Policy PR P 005*](https://objectivesag.pirsa.sa.gov.au/id%3AA307359/document/versions/published)and [*PIRSA Document and Records Management Access Controls and Security Guideline IM G 007*](https://objectivesag.pirsa.sa.gov.au/id%3AA2544/document/versions/published)(Note: the latter two PIRSA links are only accessible to SA Public Sector employees on the SA Government StateNet or PIRSA IT Networks).

Consideration should also be given to legislative provisions under the [*Public Sector (Data Sharing) Act 2016*](https://www.legislation.sa.gov.au/LZ/C/A/PUBLIC%20SECTOR%20%28DATA%20SHARING%29%20ACT%202016.aspx) and associated [*SA Office for Data Analytics Standards*](http://oda.sa.gov.au/content/data-sharing)relating to trusted access principles and data sharing safeguards, for the safe and secure sharing and use of public sector data with other departments (refer section 3.7).

## Release of open data

The [*SA Government Privacy and Open Data Guideline*](https://archives.sa.gov.au/managing-information/releasing-information-and-privacy/privacy-south-australia/privacy-guidelines-and-information-sheets) highlights the risks to privacy when considering the public release of SA Government and PIRSA datasets on the [data.sa](http://data.sa.gov.au/) and other [website](http://www.data.sa.gov.au/)s in accordance with the [*SA Government Declaration of Open Data*](https://data.sa.gov.au/strategies) and [*SA Government Open Data Toolkit and Guides*](https://data.sa.gov.au/toolkit). The SA Government is committed to government and agency data being ‘open by default’; and has directed agencies to release and publish SA Government data proactively online in accessible formats. In making SA Government data open by default, agencies must also maintain high standards of privacy in the data it releases.

The definition of ‘open data’ means **non-personal corporate data**.

**Note:** Personal information of private citizens/members of the public is **not** to be released through ‘open data’ published on the [data.sa](http://data.sa.gov.au/) and other [website](http://www.data.sa.gov.au/)s.

Examples of information to be released under the SA Government ‘open data’ program include a table of SA Government spending on infrastructure projects or a dataset consisting of geocodes for public facilities. However, other data intended for release may not have such a clear-cut distinction between non-personal and personal information, and may include de-identified personal information.

**Note:** De-identification of personal information is the removal of obscure personal identifiers and personal information so that identification of individuals that are the subject of the information is no longer possible.

PIRSA needs to ensure that its information and ICT assets maintain high standards of information security proportionate to the sensitivity of the information. This includes ensuring appropriate security classification of information in accordance with the [*SA Government Information Security Management Framework*](http://digital.sa.gov.au/resources/topic/policies-guidelines-and-standards/security/information-security-management-framework)and[*PIRSA Protective Security Policy PR P 005*](https://objectivesag.pirsa.sa.gov.au/id%3AA307359/document/versions/published) (**Note:** this PIRSA link is only accessible to SA Public Sector employees on the SA Government StateNet or PIRSA IT Networks).

Once an information privacy risk assessment and review of risk mitigation controls are undertaken, an appropriate information security classification needs to be applied to the information in accordance with the [*PIRSA Document and Records Management Access Controls and Security Guideline IM G 007*](https://objectivesag.pirsa.sa.gov.au/id%3AA2544/document/versions/published) (**Note:** this PIRSA link is only accessible to SA Public Sector employees on the SA Government StateNet or PIRSA IT Networks).

While there are significant economic, demographic and social benefits to the release of SA Government and PIRSA data, it can pose risks to the privacy of personal information. The primary risk to privacy is the identification of individuals, ie releasing data that is personal information or can be made into personal information through easily linking with other information. The harms of identification of an individual in the release of SA Government data can be significant, including:

* humiliation, embarrassment or anxiety for the individual, eg from the release of health data, it might be concluded that an individual accessed treatment for a sensitive health condition
* impacts on the employment or relationships of individuals
* affects on decisions made about an individual or their ability to access services such as their ability to obtain insurance
* financial loss or detriment
* a risk to safety such as identifying a victim of violence or a witness to a crime.

Refer to the [*SA Government Privacy and Open Data Guideline*](https://archives.sa.gov.au/managing-information/releasing-information-and-privacy/privacy-south-australia/privacy-guidelines-and-information-sheets) for further information on assessing and mitigating the risks of identification of individuals in the release of SA Government data; seeking appropriate information release approvals/consent; and methods and tools for removing identifiers/de-identifying data.

Consideration should also be given to legislative provisions under the [*Public Sector (Data Sharing) Act 2016*](https://www.legislation.sa.gov.au/LZ/C/A/PUBLIC%20SECTOR%20%28DATA%20SHARING%29%20ACT%202016.aspx) and associated [*SA Office for Data Analytics Standards*](http://oda.sa.gov.au/content/data-sharing)relating to trusted access principles and data sharing safeguards, for the safe and secure sharing and use of public sector data with other departments (refer section 3.7).

## Cloud computing technologies

The [*SA Government Privacy and Cloud Computing Guideline*](https://archives.sa.gov.au/managing-information/releasing-information-and-privacy/privacy-south-australia/privacy-guidelines-and-information-sheets) contains a non-exhaustive list of issues related to privacy and information security that an agency needs to consider and further investigate when contemplating cloud computing technologies. This is to ensure that the contract they enter into with a cloud service provider adequately addresses contactor terms and conditions relating to applicable information privacy and other obligations. This includes compliance with the information privacy principles documented in [*DPC Circular PC012*](https://www.dpc.sa.gov.au/resources-and-publications/premier-and-cabinet-circulars/DPC-Circular-Information-Privacy-Principles-IPPS-Instruction.pdf) when collecting, storing, using and disclosing personal information.

Agencies also need to ensure that they are aware of the information privacy risks and security obligations; and conduct a privacy impact assessment before entering into a contractual arrangement with a cloud computing or ICT service provider. Cloud computing poses a range of privacy issues which agencies will need to address and mitigate with appropriate legal, contractual and operational procedures as the cloud service provider assumes the function of hosting personal information.

Cloud computing privacy risks include lack of control over personal information; lack of transparency about how, where and by whom data is being stored and processed; and insufficient assessment about a cloud service provider’s location, legislative environment, operations and awareness of the potential threats and risks, and subsequent inability to mitigate those risks.

Other contract considerations that may enhance control over personal information are documented in the [*SA Government Privacy and Cloud Computing Guideline*](https://archives.sa.gov.au/managing-information/releasing-information-and-privacy/privacy-south-australia/privacy-guidelines-and-information-sheets). This includes specifying in the contract terms and conditions how, and in what format, information required to be retained will be returned to the agency at the conclusion of the contract; and how any information which is no longer required will be destroyed by the service provider in accordance with the [*State Records Act 1997*](http://www.legislation.sa.gov.au/LZ/C/A/STATE%20RECORDS%20ACT%201997.aspx).

## Websites, online applications, mobile apps and social media sites

The [*SA Government Privacy Guidelines for SA Government Websites and Online Applications*](https://archives.sa.gov.au/managing-information/releasing-information-and-privacy/privacy-south-australia/privacy-guidelines-and-information-sheets) outlines how the information privacy principles documented in [*DPC Circular PC012*](https://www.dpc.sa.gov.au/resources-and-publications/premier-and-cabinet-circulars/DPC-Circular-Information-Privacy-Principles-IPPS-Instruction.pdf) apply to agency websites; and assists agencies to develop privacy statements that explain how the agency handles any personal information collected via its websites, mobile applications (‘apps’) and social media sites.

The collection of personal information by a website, a mobile application or a social media site is not always obvious. Some information may be collected overtly, such as when an individual is asked to provide information directly. Other information may be collected covertly through the agency’s web server or through the use of cookies. It is also not always clear what will happen to the information once it is collected. It is important that users understand what information an agency is collecting about them and what the agency will do with it. This allows the user to make an informed decision about the extent to which they transact with the agency. Ultimately, being open and transparent about the way the agency handles personal information will promote trust in the agency’s practices and provide users of the agency’s website a greater level of control over how their personal information is used.

In accordance with the information privacy principles, there are a number of basic things that an agency must advise an individual before collecting that individual’s personal information. They include the purpose for collecting the information; whether the collection is authorised or required by law; and the agency’s usual practices in terms of disclosure of information. It is also good privacy practice for an agency to be as open and transparent as possible about the way in which it will handle personal information and comply with [*DPC Circular PC012*](https://www.dpc.sa.gov.au/resources-and-publications/premier-and-cabinet-circulars/DPC-Circular-Information-Privacy-Principles-IPPS-Instruction.pdf).

The agency may fulfil these obligations by publishing a clear and accessible privacy statement outlining how it will handle personal information.

The privacy statement must be both easy to find on the website and accessible to all individuals, including people with disabilities who may use assistive technology to read or hear content.

## Compliance reporting and exemptions

[*DPC Circular PC012*](https://www.dpc.sa.gov.au/resources-and-publications/premier-and-cabinet-circulars/DPC-Circular-Information-Privacy-Principles-IPPS-Instruction.pdf)mandatesPIRSA to report to the Privacy Committee of South Australia on any information the committee requires, including the action taken to ensure that the information privacy principles are implemented, maintained and observed within the agency.

Applications for exemption from compliance with the information privacy principles must be made in writing to the Privacy Committee of South Australia.

## Complaints

If a customer or member of the public believes that PIRSA may be breaching the information privacy principles, they should speak directly with PIRSA.

If PIRSA is unable to help or the customer or member of the public is dissatisfied with the response, they can lodge a complaint with the Presiding Member, [Privacy Committee of South Australia](https://archives.sa.gov.au/general-information/privacy-committee/privacy-committee-sa), GPO Box 1072, Adelaide, South Australia 5001, phone: (08) 8204 8786 or via email: staterecords@sa.gov.au. Where appropriate, the committee may refer complaints relating to privacy breaches to other bodies, such as the [Independent Commissioner Against Corruption (ICAC)](https://icac.sa.gov.au/).

Should such a complaint about PIRSA be referred to the [Privacy Committee of SA](https://archives.sa.gov.au/general-information/privacy-committee/privacy-committee-sa), the PIRSA Chief Executive (Principal Officer) is required to furnish to the committee such information as they may require to investigate the complaint.

Complaints about Australian Government agencies or private sector organisations should be directed to the [*Australian Government Office of the Australian Information Commissioner website*](http://www.oaic.gov.au/).

Refer to the [*State Records of SA Making a Privacy Complaint website*](http://www.archives.sa.gov.au/content/making-privacy-complaint) for more information.

## Data Breach response and notification processes

### Data breach response processes

As required by the [*Australian Government Notifiable Data Breaches Scheme*](https://www.oaic.gov.au/privacy-law/privacy-act/notifiable-data-breaches-scheme)*,* [*DPC Circular PC012*](https://www.dpc.sa.gov.au/resources-and-publications/premier-and-cabinet-circulars/DPC-Circular-Information-Privacy-Principles-IPPS-Instruction.pdf)and [*DPC Personal Information Data Breaches Guideline*](https://digital.sa.gov.au/resources/personal-information-data-breaches), where a known or suspected personal information data breach has been discovered, immediate response action must be undertaken, either simultaneously or in quick succession, to:

* implement appropriate measures/remedial actions to contain the data breach to prevent any further access or distribution of the affected personal information, or the possible compromise of other information
* assess the data breach by gathering the facts and evaluating the risks, including potential harm to affected individuals and, where possible, taking appropriate action to remediate any risk of harm. The [*DPC Personal Information Data Breaches Guideline*](https://digital.sa.gov.au/resources/personal-information-data-breaches) provides a list of data breach risk assessment factors that should be considered
* where the data breach is determined to be an eligible data breach which is likely to result in serious harm to any individuals whose personal information is involved in the breach, notify the relevant individuals or organisations as soon as practicable depending on the type of information involved, as described in section 3.16.3 below
* where the data breach is determined to be of low risk, determine whether the relevant individuals or organisations should be notified, as described in sections 3.16.4 and 3.16.5 below
* report, investigate and evaluate the breach in accordance with sections ‘6.7 Security incident reporting’ and ‘6.8 Security incident investigations’ of the [*PIRSA Protective Security Policy GO P 005*](https://objectivesag.pirsa.sa.gov.au/id%3AA307359/document/versions/published)*;* and [*PIRSA ICT Cyber Security Incident Reporting Procedure IM R 010*](https://objectivesag.pirsa.sa.gov.au/id%3AA88303/document/versions/published)(Note: these PIRSA links are only accessible to SA Public Sector employees on the SA Government StateNet or PIRSA IT Networks).

**Note**: ‘Serious harm’ to an individual includes serious physical, psychological, emotional, financial (including loss of business or employment opportunities) and reputational harm.

### Eligible data breach criteria

An eligible data breach arises when a breach has been assessed and meets the following three criteria:

* there is unauthorised access to or unauthorised disclosure of personal information, or a loss of personal information, that PIRSA holds, and
* it is likely to result in serious harm to one or more individuals, and
* PIRSA has not been able to prevent the likely risk of serious harm with remedial action.

If personal information is lost in circumstances where subsequent unauthorised access to, or unauthorised disclosure of the information, is unlikely, there is no eligible data breach and the processes described in section 3.16.3 are not mandated. For example, if the personal information is remotely deleted before an unauthorised person could access the information, or if the information is encrypted to a high standard making unauthorised access or disclosure unlikely, then there is no eligible data breach. Refer sections 3.16.4 and 3.16.5 for more information on notification processes and considerations in such instances.

### Eligible data breach notification process

Where an eligible data breach has been discovered, the following mandated data breach notification processes **must** be undertaken:

1. **Notification of eligible data breaches containing tax file number (TFN) information**

If an eligible data breach containing tax file number (TFN) information that connects with the identity of an individual has been discovered, PIRSA must notify the:

* PIRSA Agency Security Executive immediately
* PIRSA Chief Executive (who will determine whether the relevant Minister/s should be notified)
* individuals or organisations affected
* [Office of the Australian Information Commissioner](https://www.oaic.gov.au/privacy-law/privacy-act/notifiable-data-breaches-scheme#how-to-notify), within 30 calendar days of the breach being discovered
* [Privacy Committee of SA](https://archives.sa.gov.au/general-information/privacy-committee/privacy-committee-sa)

**Note:** the notification provided to the above individuals or organisations about TFN information must contain specific information prescribed in the [*Australian Government Notifiable Data Breaches Scheme*](https://www.oaic.gov.au/privacy-law/privacy-act/notifiable-data-breaches-scheme) and [*Australian Government Notifiable Data Breach Form*](https://forms.business.gov.au/smartforms/landing.htm?formCode=OAIC-NDB) required to be reported to the [Office of the Australian Information Commissioner](https://www.oaic.gov.au/privacy-law/privacy-act/notifiable-data-breaches-scheme#how-to-notify), including recommendations about the steps individuals should take in response to the data breach.

1. **Notification of eligible data breaches containing personal information (excluding tax file number (TFN) information)**

If an eligible data breach containing personal information **excluding** TFN information has been discovered, PIRSA must notify the:

* PIRSA Agency Security Executive immediately
* PIRSA Chief Executive (who will determine whether the relevant Minister/s are to be notified)
* individuals or organisations affected
* [Privacy Committee of SA](https://archives.sa.gov.au/general-information/privacy-committee/privacy-committee-sa).

### Low risk data breach notification process

Where a low risk breach has been discovered and it is determined that notification is required, PIRSA must notify the:

* PIRSA Agency Security Executive immediately
* PIRSA Chief Executive (who will determine whether the relevant individuals and organisations affected by the data breach and/or relevant Minister/s are to be notified)
* [Privacy Committee of SA](https://archives.sa.gov.au/general-information/privacy-committee/privacy-committee-sa).

### Other data breach notification process considerations

Notifying parties affected by a data breach is considered good practice. It can promote open and transparent government; assist in rebuilding public trust in government institutions; and enable individuals and organisations to exercise control over their personal information and security.

The decision on who and how to notify needs to be made on a case-by-case basis, dependent on the circumstances and nature of the data breach; and the outcomes of the data breach risk assessment conducted.

Consideration is to be given whether the following additional organisations need to be notified of the data breach:

* if the data breach may be a result of criminal actions, the [SA Police](https://www.police.sa.gov.au/contact-us) should be notified as soon as practicable. **Note:** Delay the notification to those affected by the data breach until advice from the SA Police is given, as notification may compromise a criminal investigation
* other law enforcement agencies, internal investigation units, across government response organisations and other regulatory bodies (including [Australian Securities and Investment Commission](http://asic.gov.au/about-asic/contact-us/), [Australian Competition and Consumer Commission](https://www.accc.gov.au/contact-us), and [Australian Communications and Media Authority](https://www.acma.gov.au/theACMA/About/Corporate/Structure-and-contacts/contact-the-acma-acma-1)), as required by relevant legislation or policy. **Note:** Where law enforcement authorities are investigating the data breach, the investigating authority must be consulted before making details of the data breach public to avoid compromising any investigation
* if the breach involves information stored or communicated electronically, the data breach must be reported as a cyber security incident to the SA Office for ICT and Digital Government Cyber Security Watch Desk (refer to sections ‘6.7 Security incident reporting’ and ‘6.8 Security incident investigations’ of the [*PIRSA Protective Security Policy GO P 005*](https://objectivesag.pirsa.sa.gov.au/id%3AA307359/document/versions/published); and the [*PIRSA ICT Cyber Security Incident Reporting Procedure IM R 010*](https://objectivesag.pirsa.sa.gov.au/id%3AA88303/document/versions/published) for more information. Note: these PIRSA links are only accessible to SA Public Sector employees on the SA Government StateNet or PIRSA IT Networks). If required, the Cyber Security Watch Desk can provide advice and assistance on the ICT aspects of managing the data breach and preventative measures
* [SA Government Chief Information Security Officer](https://digital.sa.gov.au/engage/contact-us)
* [State Records of SA](https://www.archives.sa.gov.au/content/contact-us)
* any other organisation that is the source of the information that was compromised, eg:
	+ Australian Taxation Office in the case of TFNs
	+ Medicare in the case of Medicare numbers
	+ credit card companies or financial institutions in the case of credit cards or banking information.

These organisations may be able to assist in notifying individuals or reducing the impact on those affected

* insurers such as [SAICORP](http://www.safa.sa.gov.au/contact-us#SAicorp) or others if required by contractual obligations, or to access cyber risk insurance
* other internal or external parties (eg other PIRSA business divisions, government departments, unions or other employee representatives).

Refer to the [*DPC Personal Information Data Breaches Guideline*](https://digital.sa.gov.au/resources/personal-information-data-breaches) for further guidance.

### Information to be included in data breach notifications

The information included in the data breach notification should help those affected to reduce or prevent any harm that could be caused by the breach. This includes:

* the identity of the agency
* a description of the data breach
* the type of information disclosed
* what has been done to respond to the incident and reduce harm
* assistance available to those affected and steps they can take to reduce harm
* sources of information that could assist those affected
* contact information for the agency where those affected can get more information or address concerns
* whether the incident has been notified to a regulator or other external party
* how individuals can lodge a complaint.

Where appropriate, legal advice on information to be included in data breach notifications should be obtained to ensure any legal or security implications are appropriately considered.

**Note:** An [*Australian Government Notifiable Data Breach Form*](https://forms.business.gov.au/smartforms/landing.htm?formCode=OAIC-NDB) must be completed where an eligible data breach involving TFN information must be reported to the [Office of the Australian Information Commissioner](https://www.oaic.gov.au/privacy-law/privacy-act/notifiable-data-breaches-scheme#how-to-notify).

### Reviewing existing data breach preventative measures and response processes

Following the discovery of a data breach, relevant PIRSA preventative measures and response processes (including physical, cyber, personnel and procurement security controls included in PIRSA policies, procedures, guidelines, business processes and systems) must be reviewed to prevent future breaches as part of a continuous improvement cycle.

Refer section 3.5 for further information to prevent occurrences of data breaches.

Consideration is also to be given to including the above data breach notification requirements in contracts if a service provider or other third party processes personal information, including TFN information, on PIRSA’s behalf (refer to section 3.9 for more information).

Further information on the [*Australian Government Notifiable Data Breaches Scheme*](https://www.oaic.gov.au/privacy-law/privacy-act/notifiable-data-breaches-scheme), [*Australian Government Notifiable Data Breach Form*](https://forms.business.gov.au/smartforms/landing.htm?formCode=OAIC-NDB) and other data breach notification requirements, processes and exceptions to notification obligations, can be accessed from the [*Australian Government Office of the Australian Information Commissioner website*](http://www.oaic.gov.au/)andRoles and Responsibilities

| **Role** | **Responsibilities** |
| --- | --- |
| Chief Executive | * Approving and supporting this policy.
 |
| Executive Directors | * Implementing the policy (including communication, awareness and training); and ensuring compliance with the policy by all business division employees, contractors, customers and service providers.
* Ensuring business division information custodians holding or controlling information assets containing personal information have implemented information security and privacy protocols to ensure such assets are protected and stored correctly; and that personal information is checked for accuracy before it is used or disclosed.
* Regularly reviewing and auditing the way that personal information is collected within their business divisions to ensure that the necessary controls are in place in line with the [*DPC Circular PC012*](https://www.dpc.sa.gov.au/resources-and-publications/premier-and-cabinet-circulars/DPC-Circular-Information-Privacy-Principles-IPPS-Instruction.pdf), [*SA Government Privacy Guidelines for SA Government Websites and Online Applications*](https://archives.sa.gov.au/managing-information/releasing-information-and-privacy/privacy-south-australia/privacy-guidelines-and-information-sheets)and supporting SA Government privacy guideline information sheets, and requirements of this policy.
 |
| PIRSA Freedom of Information and Privacy Officer | * Providing policy advice and assistance, including interpreting policy requirements.
* Providing advice on requests for the release, use and sharing of information which are not covered by the normal operational procedures, legislative requirements or the procedures stated in the [FOI Act](http://www.legislation.sa.gov.au/lz/c/a/freedom%20of%20information%20act%201991.aspx).
 |
| PIRSA information asset and ICT asset custodians and business owners | * Acting in accordance with this policy to ensure information privacy when dealing with personal information of customers, employees and members of the public.
* Ensuring that information assets containing personal information held, used or controlled are protected and stored correctly; and that personal information is checked for accuracy before it is collected, transmitted, solicited, published, used, shared or disclosed in accordance with this policy.
* Maintaining the security and confidentiality of information collected, transmitted, solicited, published, used, shared and accessed; and keeping appropriate records relating to provision of access to information.
* Ensuring any unnecessary personal information is removed from documents or data to be shared or distributed to external organisations or persons; or published to PIRSA websites, social media sites, online applications and [data.sa](https://data.sa.gov.au/).
* Making appropriate corrections, deletions and additions as are, in the circumstances, reasonable to ensure that information assets containing personal information are accurate, relevant, up-to-date, complete and not misleading.
* Assessing, investigating, reporting and managing any personal information data breaches in line with this policy.
* Seeking advice, if required, from the PIRSA Freedom of Information and Privacy Officer prior to the collection, transmittal, soliciting, publishing, use, sharing and disclosure of personal information.
 |
| Business Operations | * Ongoing management of the policy (including feedback, review, document and records management requirements, updating policy versions and removal of revoked policies).
* Evaluating, monitoring and reviewing the policy.
 |
| Employees, contractors, consultants and service providers | * Acting in accordance with this policy to ensure information privacy when dealing with personal information of customers, employees and members of the public.
* Making appropriate corrections, deletions and additions to information assets containing personal information as are, in the circumstances, reasonable to ensure that the information is accurate, relevant, up-to-date, complete and not misleading.
* Seeking advice, if required, from the PIRSA Freedom of Information and Privacy Officer prior to the collection, transmittal, soliciting, publishing, use, sharing and disclosure of personal information.
* Using and handling information assets gained through their employment appropriately for the purpose for which it is gathered.
* Assessing, investigating, reporting and managing any personal information data breaches in line with this policy.
* Ensuring that the privacy of individuals is maintained and to only release personal information in accordance with [*DPC Circular PC012*](https://www.dpc.sa.gov.au/resources-and-publications/premier-and-cabinet-circulars/DPC-Circular-Information-Privacy-Principles-IPPS-Instruction.pdf); the [FOI Act](http://www.legislation.sa.gov.au/lz/c/a/freedom%20of%20information%20act%201991.aspx); SA Government and PIRSA policy and guidelines; the [*Public Sector (Data Sharing) Act 2016*](https://www.legislation.sa.gov.au/LZ/C/A/PUBLIC%20SECTOR%20%28DATA%20SHARING%29%20ACT%202016.aspx) and associated [*SA Office for Data Analytics Standards*](http://oda.sa.gov.au/content/data-sharing)*;* or as otherwise lawfully permitted.
 |

# Definitions

| **Term** | **Meaning** |
| --- | --- |
| Authorised access | Means approved access to, use of, copying of, or any form of communication with, the information and data owned by an agency. |
| Clickstream data | A virtual trail of mouse clicks and activities undertaken by a user on a computer, including the trail of web user website access or links from website or page or to another automatically collected or logged. Such data may include the web user’s server address and top level domain name; the date and time of the visit to the website; the web pages accessed and documents downloaded; the previous website visited; the type of web browser used; any newsgroups the user participated in; and the email addresses of mail that a user sends and receives. |
| Cookies | A data file written to a hard drive by a website that stores information the website can use to track individual web user activities, such as passwords; login, registration or identification data; user preferences; online shopping cart information; and lists of pages visited. |
| [data.sa](http://data.sa.gov.au/) | The SA Government online data dictionary website which allows customers to search and display openly licensed SA Government data (eg facts, figures, images, spatial coordinates, statistics, system reports, tables and other products) to enable customers to transform that data to create new ideas and applications; make improved investment decisions; and facilitate research and planned service delivery. The website includes datasets available from SA Government departments, other public sector bodies and participating local government authorities. Examples of PIRSA datasets available on this website include the SA Food ScoreCard and Field Crop Production Estimates. |
| Data breach | When personal information, not already publicly available, is lost or subjected to unauthorised access, modification, disclosure/release or misuse. Data breaches may occur in a number of ways, including accidental loss; internal errors or deliberate actions of trusted employees; theft of physical assets; or the theft or misuse of electronic information such as a cyber attack.Data breaches can cause harm to the individuals whose personal information is affected. For example, a data breach could result in financial loss, or emotional distress. Examples of a data breach include when:* a laptop, tablet, USB, mobile or other ICT asset phone that holds employee or customers’ personal information is stolen or accidentally lost
* a database or application containing personal information is hacked
* someone’s personal information is sent to the wrong person.

See eligible data breach for more information. |
| De-identified data | Data where obscure personal identifiers and personal information have been removed so that identification of individuals, that are the subject of the information, is no longer possible. |
| Eligible data breach | Under [*Australian Government Notifiable Data Breach Scheme*](https://www.oaic.gov.au/privacy-law/privacy-act/notifiable-data-breaches-scheme#how-to-notify) requirements issued under the Commonwealth [Privacy Act](https://www.legislation.gov.au/Series/C2004A03712),an eligible data breach arises when the following three criteria are satisfied:* there is [unauthorised access](#Unauthorisedaccess) to or [unauthorised disclosure](#Unauthoriseddisclosure) of [personal information](#Personalinformation), or a [loss](#Loss) of personal information, that an agency holds
* it is likely to result in serious harm to one or more individuals, and
* the agency has not been able to prevent the likely risk of [serious harm](#Seriousharm) with remedial action.

Under the [*Notifiable Data Breach Scheme*](https://www.oaic.gov.au/privacy-law/privacy-act/notifiable-data-breaches-scheme#how-to-notify), if personal information is lost in circumstances where subsequent unauthorised access to or unauthorised disclosure of the information is unlikely, there is no eligible data breach. For example, if the personal information is remotely deleted before an unauthorised person could access the information, or if the information is encrypted to a high standard making unauthorised access or disclosure unlikely, then there is no eligible data breach. |
| ICT assets | Includes ICT applications, databases, equipment, infrastructure, peripherals, portable storage devices (including USBs, laptops, tablets, external hard drives, personal digital assistants, CDs, DVDs and smartphones), servers, software, cloud computing platforms and technology. |
| Information | Data to which meaning is applied by virtue of its context. It may be in physical or electronic/digital formats, including paper, scanned, stored electronically, transmitted by post or using electronic means, published online, portrayed alphanumerically or graphically, or spoken in conversation. |
| Information assets | Includes physical and electronic/digital data, documents, records, publications and web content. |
| Information subject | The person to whom the information in an information asset relates. |
| Loss | The accidental or inadvertent loss of personal information held by an entity, in circumstances where is it is likely to result in unauthorised access or unauthorised disclosure. An example is where an employee of an entity leaves personal information (including hard copy documents, unsecured computer equipment, portable storage devices containing personal information) on public transport. |
| Notifiable data breach | See [Eligible data breach](#Eligiblebreach) and [Notifiable data breach scheme](#Notifiabledatabreach). |
| [Notifiable data breach scheme](https://www.oaic.gov.au/privacy-law/privacy-act/notifiable-data-breaches-scheme#how-to-notify) | A scheme issued pursuant to the [Privacy Act](https://www.legislation.gov.au/Series/C2004A03712) which outlines relevant entity obligations to respond to data breaches. Under the scheme, relevant entities have notification obligations where eligible notifiable data breaches are likely to result in serious harm to any individuals whose personal information is involved in the breach. |
| Personal information | Information or opinion, whether true or not relating to a natural person or the affairs of a natural person whose identity is apparent, or can be reasonably ascertained, from the information or opinion (source: [*DPC Circular PC012*](https://www.dpc.sa.gov.au/resources-and-publications/premier-and-cabinet-circulars/DPC-Circular-Information-Privacy-Principles-IPPS-Instruction.pdf)). This includes combinations of name, address, date of birth, financial or health details or status, ethnicity, gender, religion, witness statements, alleged behaviours, licensing details, photographs or video footage of individuals or information subjects. It may be collected in paper form, verbally or through electronic means. |
| Portable storage devices | A small, lightweight, portable, easy to use device, which is capable of storing and transferring information and data. Common portable storage devices include, but are not limited to, portable external hard drives, CD, DVD, USB keys, flash drives, compact flash cards, SD cards, laptops/notebooks/netbooks, tablets (including iPads and Windows tablets), personal digital assistants (eg Pocket PC, Palm, BlackBerry) and devices with in-built accessible storage (eg digital cameras, iPods, iPhones and other mobile/smart phones). |
| Privacy Statement | A message or link to a statement on websites and online forms which, where applicable, specifies:* what information is collected for individuals and for what purpose
* the legal authority for the collection if it is authorised by law
* how this information is to be used; and if it is to be disclosed and to whom
* the risks to the individual of using the Internet as the transmission medium, and other options for providing information
* what clickstream data is collected, and how any cookies are used and for what purpose
* any security tools and measures (such as encryption products and level of protection provided) to be used
* details on how customers, employees and members of the public can apply for access to their own information in accordance with the [FOI Act](http://www.legislation.sa.gov.au/lz/c/a/freedom%20of%20information%20act%201991.aspx), including rights to apply to correct personal information that is out of date, incorrect or misleading.
 |
| [*SA Government Declaration of Open Data*](https://data.sa.gov.au/strategies) | A declaration by the Premier of South Australia committing the SA Government to proactively releasing data and information in accordance with international best practice. This includes making data open by default; publishing data online using agreed open standards and data formats; making data available free of charge wherever possible; openly licensing data for commercial and other reuse; and maintaining the highest standards of data and information privacy, security and integrity. |
| [*SA Government Information Security Management Framework*](http://digital.sa.gov.au/resources/topic/policies-guidelines-and-standards/security/information-security-management-framework) *(ISMF)* | A Cabinet approved framework to address SA Government information and ICT asset security. It consists of policies, standards and guidelines for use by SA Government agencies. The framework is aligned with the [*Australian Government Protective Security Policy Framework*](http://www.protectivesecurity.gov.au/Pages/default.aspx) and [*International Standard on Information Security Management ISO/IEC 27001:2005*](https://www.saiglobal.com/assurance/information-security/ISO27001.htm). |
| Serious harm | Includes serious physical, psychological, emotional, financial (including loss of business or employment opportunities) and reputational harm to an individual due to a data breach. |
| Unauthorised access | Occurs when personal information that an entity holds is accessed by someone who is not permitted to have access. This includes unauthorised access by an employee of the entity, or an independent contractor, as well as unauthorised access by an external third party (such as by hacking). For example, an employee browses sensitive customer records without any legitimate purpose, or a computer network is compromised by an external attacker resulting in personal information being accessed without authority. |
| Unauthorised disclosure | Occurs when an entity, whether intentionally or unintentionally, makes personal information accessible or visible to others outside the entity, and releases that information from its effective control in a way that is not permitted by the [Privacy Act](https://www.legislation.gov.au/Series/C2004A03712). This includes an unauthorised disclosure by an employee of the entity. For example, an employee of an entity accidentally publishes a confidential data file containing the personal information of one or more individuals on the Internet. |

# Related Docum ents

* + ***Legislation***
* [*Children’s Protection Act 1993*](http://www.legislation.sa.gov.au/lz/c/a/childrens%20protection%20act%201993.aspx)
* [*Freedom of Information Act 1991*](http://www.legislation.sa.gov.au/LZ/C/A/FREEDOM%20OF%20INFORMATION%20ACT%201991.aspx)
* [*Privacy Act 1988*](https://www.legislation.gov.au/Series/C2004A03712) *(Commonwealth)*, including the:
* [*Australian Government Notifiable Data Breaches Scheme*](https://www.oaic.gov.au/privacy-law/privacy-act/notifiable-data-breaches-scheme)
* [*Australian Government Notifiable Data Breach Form*](https://forms.business.gov.au/smartforms/landing.htm?formCode=OAIC-NDB)
* [*Australian Privacy Principles*](https://www.legislation.gov.au/Series/C2004A03712)
* [*Privacy Amendment (Notifiable Data Breaches) Act 2017*](https://www.legislation.gov.au/Details/C2017A00012)
* [*Privacy (Tax File Number) Rule 2015*](https://www.legislation.gov.au/Details/F2015L00249/Explanatory%20Statement/Text)
* [*Public Sector (Data Sharing) Act 2016*](https://www.legislation.sa.gov.au/LZ/C/A/PUBLIC%20SECTOR%20%28DATA%20SHARING%29%20ACT%202016.aspx)
* [*State Records Act 1997*](http://www.legislation.sa.gov.au/LZ/C/A/STATE%20RECORDS%20ACT%201997.aspx)
	+ ***SA Government policies, instructions and guidelines***
* [*Code of Ethics for the South Australian Public Sector*](http://publicsector.sa.gov.au/policies-standards/code-of-ethics/)
* [*SA Department of Premier and Cabinet Personal Information Data Breaches Guideline*](https://digital.sa.gov.au/resources/personal-information-data-breaches)
* [*SA Department of the Premier and Cabinet Circular PC012 - Information Privacy Principles Instruction*](https://www.dpc.sa.gov.au/resources-and-publications/premier-and-cabinet-circulars/DPC-Circular-Information-Privacy-Principles-IPPS-Instruction.pdf)
* [*SA Government Contracting and Official Records Standard*](https://archives.sa.gov.au/node/5998)
* [*SA Government Contracting and the Information Privacy Principles Information Sheet*](https://archives.sa.gov.au/managing-information/releasing-information-and-privacy/privacy-south-australia/privacy-guidelines-and-information-sheets)
* [*SA Government Declaration of Open Data*](https://data.sa.gov.au/strategies)
* [*SA Government Information Privacy Principles and Child Protection Information Sheet*](https://archives.sa.gov.au/managing-information/releasing-information-and-privacy/privacy-south-australia/privacy-guidelines-and-information-sheets)
* [*SA Government Information Security Management Framework*](http://digital.sa.gov.au/resources/topic/policies-guidelines-and-standards/security/information-security-management-framework)
* [*SA Government Information Sharing Guidelines for Promoting Safety and Wellbeing*](https://www.dpc.sa.gov.au/__data/assets/pdf_file/0009/45396/Information-Sharing-Guidelines.pdf)
* [*SA Government Model Terms and Conditions Clauses for the Information Privacy Principles and Records Management*](https://archives.sa.gov.au/sites/default/files/documentstore/policies-guidelines/Guideline/model_terms_and_conditions_-_ipps_and_records_management.pdf)
* [*SA Government Open Data Toolkit and Guides*](https://data.sa.gov.au/toolkit)
* [*SA Government Photographic Images and Privacy Information Sheet*](https://archives.sa.gov.au/sites/default/files/documentstore/policies-guidelines/Advice%20Sheet/photographic_images_and_privacy_-_information_sheet.pdf)
* [*SA Government Privacy and Cloud Computing Guideline*](https://archives.sa.gov.au/managing-information/releasing-information-and-privacy/privacy-south-australia/privacy-guidelines-and-information-sheets)
* [*SA Government Privacy and Open Data Guideline*](https://archives.sa.gov.au/managing-information/releasing-information-and-privacy/privacy-south-australia/privacy-guidelines-and-information-sheets)
* [*SA Government Privacy Guidelines for SA Government Websites and Online Applications*](https://archives.sa.gov.au/managing-information/releasing-information-and-privacy/privacy-south-australia/privacy-guidelines-and-information-sheets)
* [*SA Office for Data Analytics Data Sharing Request and Approval Forms*](http://oda.sa.gov.au/content/data-sharing)
* [*SA Office for Data Analytics Standards and Guidelines*](http://oda.sa.gov.au/content/data-sharing)
	+ ***PIRSA policies***

**Note:** the following PIRSA links are only accessible to SA Public Sector employees on the SA Government StateNet or PIRSA IT Networks:

* *PIRSA intranet > Tools & Services >* [*Information Privacy*](http://intranet.pirsa.sa.gov.au/work_tools/information_privacy) *site*
* *PIRSA intranet > Documents > Forms & Templates >* [*Media, Communications, Marketing and Engagement*](http://intranet.pirsa.sa.gov.au/documents/forms_and_templates/media_communications_marketing_publishing) *site* – to access photography and video consent forms for adults and children
* [*PIRSA Document and Records Management Access Controls and Security Guideline IM G 007*](https://objectivesag.pirsa.sa.gov.au/id%3AA2544/document/versions/published)
* [*PIRSA Document and Records Management Policy IM P 002*](https://objectivesag.pirsa.sa.gov.au/id%3AA49559/document/versions/published)and [associated guidelines](http://intranet.pirsa.sa.gov.au/policies_and_procedures/document_and_records_management/guidelines_5)

* *[PIRSA ICT Cyber Security Incident Reporting Procedure IM R 010](https://objectivesag.pirsa.sa.gov.au/id%3AA88303/document/versions/published)*
* [*PIRSA Information and ICT Management Policy IM P 001*](https://objectivesag.pirsa.sa.gov.au/id%3AA3743/document/versions/published)
* [*PIRSA Information and ICT Security Policies, Procedures and Guidelines*](http://intranet.pirsa.sa.gov.au/documents/policies_and_procedures/ict_helpdesk/security_and_policies)
* [*PIRSA Protective Security Policy PR P 005*](https://objectivesag.pirsa.sa.gov.au/id%3AA307359/document/versions/published)