



**ACT**  
Government

---

Justice and Community Safety

## Privacy Policy

JACS Policy Number:

JACS POL 09

Endorsed by:

Executive Management Council

Authorised by the Director-General:



---

Director-General

Date Endorsed:

17 April 2015

## Document Properties

### Approval

Document Properties	Approval Details
Date Approved:	April 2015
Date Effective:	April 2015
Approved version:	v.4
Approved by:	Director General
Review Date:	Ongoing, with a formal review to be undertaken no later than August 2016
Expiry Date:	N/a

### Amendment History

Version No	Issue Date	Details	Author
v.1	August 2014	Initial draft	Alex Jorgensen-Hull
v.2	August 2014	Final draft	Lauren Callow
v.3	September 2014	Revised final draft – modifications to email item	Danielle Krajina
v.4	October 2014	Amendments made in accordance with OAIc advice / Amendments made following administrative changes	Alex Jorgensen-Hull Lauren Callow

### Details

Document Properties	Details
Policy Name:	Privacy Policy
Policy Number:	JACS POL 09
Policy Type:	Governance
Custodian:	Executive Director Governance
Policy Advisor:	Senior Information Officer
Branch Responsible for the Policy:	Governance
Stakeholders:	All JACS Employees
Document Location:	
File Number and Name:	JACS POL 09 Privacy Policy
Document References and/or Legislation:	<i>Information Privacy Act 2014</i> <i>Public Sector Management Act 1994</i> <i>Territory Records Act 2002</i> <i>Health Records (Privacy and Access) Act 1997</i> ACT Government Web Privacy Policy JACS Service Charter JACS Complaints Policy

## Contents

1. Purpose.....	4
2. Policy Statement.....	4
3. Remaining anonymous.....	5
4. Collection of your personal information.....	5
5. How do we collect personal information.....	5
6. Types of information we collect and hold.....	6
7. Notice of collection .....	7
8. Collecting through our websites .....	7
9. Social Networking Services .....	7
10. Email lists.....	8
11. Use and disclosure of personal information.....	8
12. Sharing information with service providers.....	10
13. Disclosure of personal information overseas .....	10
14. Quality of personal information .....	10
15. Storage and security of personal information.....	11
16. Accessing your personal information .....	11
17. Correcting your personal information .....	12
18. How to make a complaint.....	12
18.1 How to contact us .....	12
19. Compliance with this Policy .....	13
20. Review .....	13
Attachment A.....	14

## 1. Purpose

This Privacy Policy sets out how the Justice and Community Safety Directorate (the Directorate) manages personal information when performing its functions.

The specific legal obligations of the Directorate when collecting and handling your personal information are outlined in the *Information Privacy Act 2014* and in particular, in the Territory Privacy Principles found in the Act.

This statement is made in accordance with Territory Privacy Principle 1.3 of the Information Privacy Act.

Access the [Information Privacy Act](#)

We will update this Privacy Policy when our information handling practices change. Updates will be published on our website.

View the [ACT Government Web Privacy Policy](#)

## 2. Policy Statement

The Directorate collects, holds, uses and discloses personal information to carry out functions or activities under the *Public Sector Management Act 1994*, the *Territory Records Act 2002*, the *Freedom of Information Act 1989* and a number of other pieces of legislation relating to justice and criminal law, civil, commercial and property law, community safety and regulatory laws.

These functions and activities include:

- Administering ACT laws relating to justice, criminal, civil, commercial, property and community safety law.
- Handling privacy and other complaints.
- Responding to information access requests, including FOI requests.
- Providing advice to the Chief Minister, the Attorney-General, the Minister for Justice and the Minister for Police and Emergency Services on issues relating to justice and criminal law, civil, commercial and property law, regulatory and community safety laws.
- Consulting with stakeholders, for example, on reviews of legislation and inquiries into issues of public concern.
- Maintaining registers where required by legislation or where needed to perform legislative functions.
- Communicating with the public, stakeholders and the media including through websites and social media.
- Administration of employees, such as the appointment of officers and management of personnel.

The Directorate's functions are determined by the [Administrative Arrangements](#) which can be found on the ACT Legislation Register.

Please note, the Information Privacy Act does not extend to personal health information. All health records held by the Directorate are protected and managed in accordance with the *Health Records (Privacy and Access) Act 1997*.

### **3. Remaining anonymous**

Wherever possible when dealing with the Directorate (for example, when calling on the phone to make an enquiry) you will have the option of remaining anonymous or using a pseudonym (a made up name).

However, in some situations the Directorate will need you to provide your name or other details in order to provide services or assistance to you, including if we are authorised or required by law to deal with an identified individual. If in doubt, please discuss the issue with the person with whom you are dealing.

If it is impracticable or unlawful for us to deal with you without you providing identifying information, we will let you know why we need your personal information and what it will mean for you if the information is not collected.

### **4. Collection of your personal information**

At all times, the Directorate tries to only collect personal information where that information is reasonably necessary for, or directly related to, one or more of our functions or activities.

Normally the Directorate will only collect sensitive information (such as sexual orientation or criminal record) with your consent or as required by law.

Sometimes however, we may collect personal information without your consent, such as when it is required or authorised by a law, or court or tribunal order, or is necessary to prevent a threat to the life, health or safety of one or more individuals, or to public health or safety.

The Directorate will not collect personal information about you if we do not need it.

### **5. How do we collect personal information**

The Directorate will only collect information by lawful and fair means.

The main way the Directorate collects personal information about you is when you give it to us.

Your personal information may be collected in a variety of ways, including through paper or online forms, in correspondence to and from you as well as email, over the telephone and by fax.

The Directorate collects personal information when:

- We are required or authorised by law or a court or tribunal order to collect the information.
- You participate in community consultations, forums or make submissions to us, and you consent to our collection of your personal information.
- You contact us to ask for information (but only if we need it).

- You ask for access to information that the Directorate holds about you or other information about the operation of our business.

We may also collect contact details and some other personal information if you are on our committees or participating in a meeting or consultation with us.

Normally we collect information directly from you unless it is unreasonable or impracticable to do so. In certain circumstances, for example where it is required by law, we may also obtain information collected by other Australian, state and territory government bodies or other organisations. We may also receive information from a third party where this is necessary to fulfil our legislative responsibilities (i.e. emergency services).

We also collect personal information from publically available sources where that is reasonably necessary for, or directly related to our functions. For example we collect personal information from publicly available sources to enable us to engage with stakeholders who may be interested in our consultations or support research that we carry out.

## 6. Types of information we collect and hold

The Directorate endeavours to collect the minimum amount of personal information that is required to perform its functions. The personal information we collect and hold will vary depending on what we require to perform our functions and responsibilities. It may include-

- Information about your identity (e.g. date of birth, country of birth, passport details, visa details and drivers licence).
- Your name, address and contact details (e.g. phone, email and fax).
- Information about your personal circumstances and associations (e.g. age, gender, marital status and occupation).
- Information about your financial affairs (e.g. payment details, bank account details, and information about business and financial interests).
- Information about your employment (e.g. applications for employment, work history, referee comments and remuneration).
- Information about assistance provided to you under our assistance arrangements.

Sensitive information is handled with additional protections under the Information Privacy Act.

The Directorate will not normally collect sensitive information about you without your consent, unless this is required by law or another exception applies.

The Directorate holds sensitive information about the criminal records of its employees, as a standard ACT Public Service requirement.

It also holds the following sensitive personal information where it is relevant to the management of a custodial facility or court proceeding:

- criminal record
- biometric information
- racial or ethnic origin

- religious beliefs.

The Directorate does not generally collect or hold other types of sensitive information such as:

- philosophical beliefs
- political opinions
- membership of a political association
- membership of a professional or trade association
- membership of a trade union
- religious beliefs
- sexual orientation and practices
- genetic information.

## 7. Notice of collection

When the Directorate needs to collect personal information from you, we will take all reasonable steps to notify you about<sup>1</sup> -

- Who we are and how you can contact us.
- The circumstances in which we may or have collected personal information.
- The laws that requires us to collect this information (if any).
- How you may be affected if we cannot collect the information we need.
- The details of any agencies or entities which we normally share personal information with, including whether those recipients are overseas, and which countries those recipients are located in.
- The existence of this Privacy Policy explaining how we handle your information, how you can access or request changes to your personal information, and how we deal with complaints about our information handling.
- How you can access the Directorate's Privacy Policy.

## 8. Collecting through our websites

View the [ACT Government Web Privacy Policy](#)

## 9. Social Networking Services

If you communicate with the Directorate using social networking services like Facebook or Twitter, your information may also be collected by those social networking services in accordance with their own privacy policies. The Directorate may have limited or no control over the ways in which your information might be used or disclosed by those services.

---

<sup>1</sup> Note, an exemption applies to forms and court documents managed by the ACT Courts and Tribunals

## 10. Email lists

If you subscribe to a Directorate email list (refer **Attachment A**), your details will be collected for the purposes of that subscription list. If you no longer wish to subscribe, it is necessary for you to request that you be unsubscribed. Instructions on how to do this can be found at Attachment A.

## 11. Use and disclosure of personal information

The Directorate uses and discloses personal information to allow the Directorate to perform its functions effectively.

Common situations in which the Directorate will disclose information are detailed below.

### Referring information to another ACT Government Directorate or agency

The Directorate will share information with other ACT agencies in situations where you would reasonably expect us to use the information for that purpose.

- **Correspondent personal information** - if you write to us with a question, inquiry or request for assistance and we are not able to answer it fully or provide assistance we would disclose your name, contact details and the nature of your question, inquiry or request for assistance to the ACT agency that is best placed to assist you.
- **Cross agency programs** - if you participate in a program that is administered or involves more than one ACT, Commonwealth or state government agency (i.e. Farm Fire Wise) we may disclose your name, contacts, and details of your participation in the program with these other stakeholder agencies.
- **Consultation and survey records** - if you participate in meetings, policy consultations or make submissions or representations to us, we may disclose information about your name, occupation, professional or organisational associations, and your views with respect to the issue, to other ACT agencies and stakeholders.
- **Complaints information** - if you complain about a JACS policy, decision or action the personal information we might share could include your contact details, use of appeal or review mechanisms, complaint and/or customer reference numbers with any other agency, how the action complained about has affected you, and any outcome you would like to obtain. This information may be disclosed to the ACT Ombudsman to enable the Ombudsman to independently investigate the complaint.
- **Personnel records** - Personnel files are kept to maintain records about all aspects of employment including recruitment, employment history, payroll, leave, equal employment opportunity data, workplace relations, security clearances, performance, workplace health and safety, rehabilitation and compensation. These records are kept in relation to all permanent, contracted and temporary staff members/employees. Personal information is disclosed on a 'need to know' basis to Shared Services for the purposes of administering our payroll, and to travel providers under the 'whole of government' travel arrangements.

- **FOI Records** - The purpose of these records is to record all requests for information made to the Directorate under the Freedom of Information Act 1989. Personal information on these records may relate to the person who has made the FOI request, Directorate staff, staff of other agencies, and any other person whose personal information is contained in the record to which FOI access has been sought. Depending on the information contained in the records, these may be released to relevant ACT agencies.

### **Disclosure to the media**

The Directorate will only provide the media with your personal information with your consent, where such information is already publically available, or where a specific exception under the Act applies (see below for further information on exceptions).

### **Disclosure of sensitive information**

The Directorate will only disclose your sensitive information for the purposes for which you gave it to us or for directly related purposes you would reasonably expect or if you agree.

### **Exceptions**

The Directorate will not use your personal information for a secondary purpose or share your personal information with private sector organisations or anyone else without your consent, unless an exception applies.

Exceptions are available under a number of circumstances including when –

- The use or sharing of information is legally required or authorised by a law, or court or tribunal order.
- The collection is reasonably necessary for a law enforcement related activities, such as the prevention, detection, investigation, prosecution or punishment of criminal offences or breaches of the law, intelligence gathering, surveillance, conduct of protective or custodial services. Information collected by emergency services personnel (i.e. the ACT Ambulance Service) for instance, may be supplied to ACT Policing where this is required as part of an investigation into to a possible breach of the law.
- We reasonably believe that collection is necessary to lessen or prevent a serious threat to the life, health or safety of any individual, or to public health or safety.
- We have reason to suspect unlawful activity, or misconduct of a serious nature, that relates to our functions and we reasonably believe that collection of the information is necessary in order for us to take appropriate action.
- We reasonably believe that the collection is reasonably necessary to help locate a person who has been reported as missing.

If the Directorate has this information, it is allowed to provide your biometric information (such as your fingerprints or photograph) or your biometric templates (digital representations of your distinct characteristics) to an enforcement body (like the Australian Federal Police or the Department of Immigration) if we comply with any guidelines made by the Information Privacy Commissioner.

The Directorate may also disclose personal information to Commonwealth intelligence agencies where that disclosure is authorised by the head of the intelligence agency and the agency certifies that the collection of the personal information from the Directorate is necessary for its functions.

## **12. Sharing information with service providers**

The Directorate will contract service providers to support it in carrying out specific activities and functions. In some circumstances it may be necessary for the Directorate to share personal information with these service providers to enable them to perform their functions efficiently and effectively.

In these situations we protect personal information by only entering into contracts with services providers who agree to comply with Territory requirements for the protection of personal information.

## **13. Disclosure of personal information overseas**

In some circumstances, the Directorate may need to share or store information with overseas recipients.

The Directorate currently has arrangements in place to disclose personal information overseas to:

- allow analysis of that information by contracted service providers based in America. Web traffic information is disclosed to Google Analytics when you visit our websites. Google stores information across multiple countries.

As noted above, when you communicate with us through a social network service such as Facebook or Twitter, the social network provider and its partners may collect and hold your personal information overseas.

If disclosure of personal information overseas is necessary we will take reasonable steps before disclosing the information to ensure that the recipient treats the personal information with a similar standard of care as is required by the Information Privacy Act.

In some cases, the information will already be sufficiently protected under the law governing the overseas recipient and you can access mechanisms to enforce these protections.

If it is practical and reasonable to do so, we will obtain your consent to overseas disclosure. However there may be situations where we are unable to do so (for example, where we share information as part of a law enforcement activity). In this situation, the Directorate will take all reasonable steps to ensure the overseas recipient complies with the requirements of the Information Privacy Act.

The Directorate will ensure this Privacy Policy is updated to reflect any new arrangements it may enter into resulting in the regular sharing of personal information with an overseas recipient.

## **14. Quality of personal information**

The Directorate is required to take reasonable steps to ensure that the personal information we collect is accurate, up to date and complete.

To ensure that the personal information we collect is accurate, up-to-date and complete we record information in a consistent format; and where necessary, confirm the accuracy of information we collect from a third party or a public source.

Personal information we use or disclose must be relevant for the purpose for which we use or disclose it.

## **15. Storage and security of personal information**

The Directorate is required to take reasonable steps to ensure that personal information it holds is safe and secure. Every effort is taken to protect your personal information from misuse, interference or loss from unauthorised access, use, modification or disclosure in accordance with the Information Privacy Act.

The *Territory Records Act 2002* establishes frameworks for the management of your personal information if it is held within the files or data systems of the Directorate. The Directorate will also handle your personal information in accordance with any requirements set out by the legislation under which it was collected.

Our IT systems employ protections to guard against unauthorised access. Paper based files are stored securely and access to Directorate premises is controlled.

As part of our general practice, personal information is only made available to staff who have a need to access it in order to perform their role.

Information will be securely destroyed once it is no longer required for business purposes in accordance with the requirements of the Territory Records Act 2002 and the approved Record Disposal Schedules as listed in the Directorate Records Management Program.

## **16. Accessing your personal information**

In accordance with the Information Privacy Act (Territory Privacy Principle 12) you have the right to ask for access to personal information that the Directorate holds about you.

If you contact us to request access to your personal information, we must provide you with access to information in the way you request, if it is reasonable and practical to do so. The Directorate may refuse you access to the document if an exception in TPP 12.2 applies or if it is not reasonable or practicable to give you access in the way you request, we must take reasonable steps to give access in a way that meets both our needs and your needs.

The Directorate must respond to your request in writing within 30 days. If we refuse your request, we must tell you why we are unable to provide you with access to that information.

We will not charge you any fees for making the request or providing you with access, unless a fee has been specifically determined for the information in question (i.e. births, deaths and marriages information).

You also have the right under the *Freedom of Information Act 1989* to request access to documents that we might hold. Further information on the Directorate's freedom of information arrangements, including how you can apply for access, can be found [on the JACS Directorate website](#).

## 17. Correcting your personal information

Under the Information Privacy Act (Territory Privacy Principle 13) you may also request that we correct any of your personal information that we might hold, if you believe it is incomplete, incorrect, out of date or misleading.

If you ask the Directorate to correct your personal information, we must take reasonable steps to correct the information if we are satisfied that it is incorrect, inaccurate, incomplete, irrelevant, out of date or misleading.

If we agree to correct information and that information has previously been shared with another agency, you may request that we notify the other agency of the possible need for them to correct that information.

There may be reasons why we refuse to correct that information, for example, if we are required or authorised by law not to correct the information.

If we refuse to correct the information, we must give you written notice of why we have refused to correct your information and how you may complain about our decision, within 30 days.

If we refuse to correct your personal information, you can ask us to attach or link a statement that you believe the information is incorrect to the information.

We will not charge you any fees for making the request for correction, correcting the information or attaching a statement to the personal information.

## 18. How to make a complaint

Access a copy of the Directorate's [Complaint Policy](#)

Complaints about the Directorate's handling of your personal information should be made in writing to the contact details below. We are also able to assist you to lodge your complaint if required. Please also contact us if you would like to request a hard copy of the privacy policy.

We will consider your complaint to work out how we can resolve your issue satisfactorily. We will endeavour to acknowledge receipt of your complaint within five working days and respond to the complaint within 21 days.

If you are not satisfied with our response, you may ask for a review by a more senior officer or you can make a formal privacy complaint to the Information Privacy Commissioner under section 34 of the Information Privacy Act.

The Information Privacy Commissioner is an independent body that will assess your complaint and can make a determination that our actions are an interference with your privacy. Note, some of the functions of the Information Privacy Commissioner for the ACT are currently being performed by the Australian Information Commissioner, including the handling of complaints against ACT public sector agencies. If your complaint is upheld by the Commissioner, you may be able to seek a remedy in the Magistrates Court. The Commissioner can be contacted on 1300 363 992 or via the website at [www.oaic.gov.au](http://www.oaic.gov.au).

### 18.1 How to contact us

You can contact us by:

**Email:** [JACSEnquiries@act.gov.au](mailto:JACSEnquiries@act.gov.au) or [JACSComplaints@act.gov.au](mailto:JACSComplaints@act.gov.au)

**Telephone:** 02 6207 4813

**Post:** GPO Box 158  
Canberra ACT 2601

### **Assisted Contact**

#### **National Relay Service:**

- TTY users phone – 133 677, then ask for 13 22 81
- Speak and listen users – 1300 55 727, then ask for 13 22 81
- Internet relay users – connect to the National Relay Service and ask for 13 22 81

#### **Translating and Interpreting Service:**

- Call 13 14 50

## **19. Compliance with this Policy**

Business units will be routinely audited in relation to their compliance with this policy.

## **20. Review**

This policy will be reviewed on an ongoing basis, with a formal review to be undertaken at least every two years.

## **Attachment A**

The Directorate does not currently manage any subscriber email lists.