Right to Information – Preventing and responding to the inadvertent release of personal information

1. Purpose

This document provides guidance for Right to Information (RTI) delegated officers in the Department of Justice (the Department) on actions to prevent the accidental or mistaken release of personal information in response to RTI applications and the actions to be taken where there has been an inadvertent release.

While this guidance has been developed to provide a consistent and practical framework for preventing and responding to such incidents, it is acknowledged that each situation will vary. RTI delegated officers should therefore exercise judgement and, where a potential inadvertent release of personal information is identified take immediate steps to limit any further access or distribution of the personal information.

Additional information in relation to assessing the level of harm, notifying managers and affected individuals is outlined below.

This guideline does not cover breaches of information related to cyber-security, intentional staff misuse or release of personal information. All queries relating to these issues should be directed to the Chief Information Security Officer.

2. Responsibility of all staff

All staff have a responsibility to take reasonable steps to prevent the accidental or unauthorised disclosure of information.

RTI delegated officers should carefully check for personal information that is exempt under the *Right to Information Act 2000* (RTI Act) and ensure responses to right to information applications are quality assured by another staff member before release. If there is any uncertainty about whether the information is personal information or if it can be disclosed, RTI delegates should seek advice from their manager or another RTI delegated officer before releasing the information.

All RTI delegated officers are required to comply with this guidance, and any related policies or legislation.

3. What is personal information?

The *Personal Information Protection Act 2004* (PIP Act) and RTI Act define personal information as:

> *Any information or opinion in any recorded format about an individual –*
>
> > *(a) whose identity is apparent or is reasonably ascertainable from the information or opinion; and*
> >
> > *(b) who is alive or has not been dead for more than 25 years.*

This may include, but is not limited to, a person's full name, date of birth, age, residential address, family members, phone number and email address.

Sensitive personal information includes information about an individual's:

- racial or ethnic origin
- political opinions
- membership of a political association
- religious beliefs or affiliations
- philosophical beliefs
- membership of a professional or trade association
- membership of a trade union
- sexual orientation
- criminal record
- health information.

4. Personal information protection principles

Schedule 1 of the PIP Act lists the personal information protection principles that apply in Tasmania. It is recommended that RTI delegates make themselves familiar with these principles.

For the purposes of this guidance document, the following principles also apply:

- any inadvertent release of personal information, however minor, **must be treated seriously and acted on immediately**
- the response should be proportionate to the level of risk and harm
- where practicable and appropriate, affected individuals should be informed
- all incidents should be reviewed with a view to process improvements.

5. What is an inadvertent release?

An inadvertent release occurs where personal information is disclosed unintentionally. Examples include but are not limited to:

- sending an email containing personal information to the wrong recipient
- failing to redact exempt information (e.g. under s36 of the RTI Act)

- attaching the wrong version of file
- accidental publication of personal information on the Department's Disclosure Register.

6. Preventing an inadvertent release

RTI delegated officers should always follow the Department's RTI Policy and RTI procedures and carefully consider information that may be exempt under the RTI Act.

When dealing with RTI applications that include personal information, additional considerations may apply to prevent the accidental release of confidential information relating to individuals other than the applicant.

In addition to reading and identifying personal information for redaction manually, RTI delegated officers should:

- undertake an electronic search within documents for relevant personal information identified through the manual process to ensure that all instances have been identified and redacted (noting that certain document types, including scanned materials and handwritten notes, may not be readable and therefore not identified by the relevant software)
- have another RTI delegate or staff member check that all personal information has been identified
- apply clear naming conventions to all RTI files in the Department's records system (e.g. 'UNREDACTED', 'DRAFT' or 'FINAL')
- double check the correct file or version of a file is attached when sending information electronically to applicants
- carefully consider whether information is appropriate for release on the Department's Disclosure Register before publication and seek additional advice if required.

RTI delegated officers should also consider additional review and quality assurance processes if an application involves the release of particularly sensitive information, e.g. information relating to children and young people, victim-survivors or other sensitive information as defined under the PIP Act.

7. Immediate actions to be taken

RTI delegated officers must take the following steps as soon as a potential inadvertent release is identified.

7.1. Contain the release

If it is reasonable and practicable in the circumstances, steps should immediately be taken to contain the inadvertent release of personal information. Examples of such steps include attempting to recall an email that was sent to an incorrect recipient,

emailing an incorrect recipient advising of the error and requesting the email be deleted or immediate removal of the information from the Disclosure Register.

7.2. Report immediately

RTI delegated officers should immediately notify their manager of the inadvertent release to determine what next steps should be taken.

Depending on the amount and nature of information that has been released, it may also be appropriate to inform the following departmental officers:

- the RTI delegated officer's Output Manager
- the information custodian, i.e. the Output Manager who provided the data to the RTI delegated officer
- Deputy Secretary/Secretary
- Director, Strategic Communications
- Chief Information Security Officer.

In the case of a breach that may cause serious harm to an individual or group, consideration should also be giving to advising the relevant Minister.

7.3. Document the incident

As soon as practicable after becoming aware of an inadvertent release, the circumstances surrounding the release should be documented. Depending on the severity of the inadvertent release, this may take the form of an email to the relevant manager outlining the release and what remedial action was taken (or is intended to be taken), or for more serious inadvertent releases, a detailed briefing to the Output Manager, Deputy Secretary/Secretary or relevant Minister may be required.

At a minimum, the following details should be documented:

- when the inadvertent release occurred
- what information was disclosed
- who the information was disclosed to
- how the inadvertent release occurred
- what remedial action has been taken (or is intended to be taken) and whether the incident has been contained
- any suggested actions to prevent such a release recurring in the future.

Where these details are not immediately available, they should be added as needed once obtained.

All documentation relating to an inadvertent release should be stored in the Department's record management system (Content Manager) against the relevant RTI folder.

8. Assessment of severity

The RTI delegate and responsible manager should assess the level of harm caused by the inadvertent release as **Minor** or **Serious** based on, but not limited to, the following factors:

Factor	Considerations
Sensitivity	Was it sensitive personal information? (Refer section 2 for a list of information that is considered sensitive.)
Volume	The number of individuals affected
Identifiability	Can individuals be readily identified?
Recipient	Was the recipient internal, external, known, trusted?
Likelihood of misuse	Risk of harm (e.g. risk of identity theft, distress, reputational damage, harassment, physical harm or economic harm)
Ability to contain	Has the information been recovered or secured, who has access to the information, or is it still being shared or disclosed?

Minor inadvertent releases will have limited impact and be low risk in nature. Examples of minor inadvertent releases include a RTI response with limited personal information and low sensitivity sent to a known recipient, who confirms deletion.

Serious inadvertent releases have potential for greater harm. Examples of more serious inadvertent releases include an email with an attached spreadsheet of multiple client details or sensitive personal information of an individual. A serious inadvertent release may also include disclosure to unknown or external parties or the inability to confirm deletion or containment.

Special consideration may also apply to the release of personal information relating to individuals involved in the criminal justice system (i.e. the inadvertent release of personal information to a prisoner that includes the personal information of another prisoner or a victim of crime).

9. Response actions - Minor inadvertent release

If the inadvertent release is considered to be minor, appropriate steps may include:

- immediate containment and reporting
- documenting the inadvertent release and remedial actions
- reviewing processes and procedures to reduce the risk of a similar incident recurring

- notification to individuals may not be required but should be considered by appropriate officers.

10. Response actions - Serious inadvertent release

If the inadvertent release is considered to be serious, appropriate steps may include:

- immediate containment and reporting
- documenting the inadvertent release and any remedial actions taken or planned to be taken
- Escalation to relevant senior staff of the Department, e.g. the Output Manager, Deputy Secretary, Secretary, Chief Information Security Officer, Manager, Communications, Director of Prisons, Minister
- consideration of whether legal advice is required
- informing the affected individual/s (refer to section 11 for additional information regarding what to include in communication to affected individuals)
- undertaking a structured incident assessment to identify the cause of the inadvertent release and what actions should be taken to reduce the likelihood of a recurrence (example actions may be amending policies or procedures, additional staff training, naming conventions, building safeguards into technology to identify personal information)
- external reporting as appropriate (e.g. depending on the circumstances it may be appropriate to advise the Ombudsman, police or law enforcement agency or other external bodies of the inadvertent release).

11. Informing affected individuals

Individuals affected by a serious inadvertent release of personal information should be notified as soon as possible. Such notification may include:

- advice that personal information has been disclosed and an explanation of what information has been released
- the circumstances of the release
- who has obtained or is likely to have obtained access to the information
- the steps taken to contain the inadvertent release (it might also be appropriate to explain what future steps will be taken)
- any recommended actions that the affected individual/s should take, e.g. changing passwords
- an apology and advice of their right to complain under the PIP Act
- contact details for further information.

In the case of an inadvertent release involving multiple individuals, consideration may also need to be given to a public notice.

All communication with individuals affected by a serious inadvertent release of personal information should be approved by the relevant Deputy Secretary or Secretary before being finalised and sent.

12. Related Guidance

The following sources provide additional information with respect to the collection, storage, use and release of personal information:

- *Right to Information Act 2009*
- *Personal Information Protection Act 2004*
- OAIC Data Breach Response Guidance
- Department of Justice Right to Information – Information Disclosure Policy
- Department of Justice Right to Information – Information Disclosure Procedures

---

Responsible Output: Office of the Secretary

Version number: 1.0

Version approved: 24/08/2026

Next review date: 24/08/2029