Right to Information and Privacy

Management of Technical (low level) Privacy Breaches Procedure

1. About this procedure

The *Management of Technical (low level) Privacy Breaches Procedure* sets out the process for managing a minor breach received within business units of the Department of Justice and Attorney-General (DJAG).

2. Background

The level of privacy reporting has significantly increased due to the privacy awareness and training programs undertaken throughout DJAG.

A significant portion of this reporting are low level privacy issues (technical breaches) that have limited to no impact on the individual whose personal information it relates to.

This procedure outlines when to deal with a low level technical privacy breach in a business unit and report the outcome to Right to Information (RTI) and Privacy (privacy@justice.qld.gov.au) and when to refer the assessment of the privacy breach to RTI and Privacy.

3. Application

This procedure applies to all employees of DJAG who receive a notice of a potential privacy breach from an officer of DJAG or who are submitting a self-reported privacy breach. This procedure is to be used in conjunction with: the *Client complaint management policy;* the *Employee complaints management policy*; *Information Privacy: Complaints and Breaches Investigation Policy*; *Information Privacy: Complaints and Breaches Investigation Procedure*; *Information Privacy: Breach and Complaint Assessment Triage Form*; and any relevant departmental guidelines.

This procedure outlines the process for managing **low level privacy breaches about a DJAG service, practice, or DJAG officer's action/activity when providing a service.**

Examples of technical (low level) privacy breaches could be, but are not limited to:

- a document containing personal information being attached to an incorrect system account file e.g. MACS (Marketplace Accreditation and Compliance System) used by the Office of Fair Trading, where no reliance or decision has been made on the incorrect information and no disclosure of the incorrectly attached document has subsequently been made in error.
- information regarding an officer attached to another officer's hardcopy file, providing it has not been used to support a decision and providing no subsequent disclosure of the incorrectly attached information occurs.
- an email regarding an individual sent to an incorrect person, but still within DJAG, and where written confirmation advice has been received that the email has been deleted from the incorrect recipient's inbox and deleted items folder.

4. Roles and responsibilities

Receiving officer (can be any DJAG employee)
• Receives advice of potential privacy breach from departmental notifier or the self-notifier and refers to business unit manager.
• Business unit manager, or officer nominated by the business unit manager, reviews circumstances surrounding the privacy breach and undertakes a self-assessment (using the Privacy Breach Checklist – see below and Appendix 1).
• Business unit manager, or officer nominated by the business unit manager, in consultation with relevant officers, resolves low level breaches.
• The business unit manager, or officer nominated by the business unit manager, reports the matter and remedial action taken to privacy@justice.qld.gov.au for further assessment by RTI and Privacy.
Managing officer (RTI and Privacy)
• Receives and assesses the circumstances surrounding the privacy breach.
• Advises the business unit manager, or officer nominated by the business unit manager, in writing of the provisions that were technically contravened and whether immediate closure is recommended.
• Requests additional information be provided to RTI and Privacy for further assessment.
• Notes details of privacy breach to be recorded in internal CMS database and included in weekly report to senior management.
Business unit manager, or officer nominated by the business unit manager
• As required, the business unit manager provides additional information requested by RTI and Privacy for further assessment.
• Provides copy of the low level incident to the divisional contact officer (refer to intranet page – yet to be updated, in the interim contact RTI and Privacy).

5. Privacy Breach Checklist

To assist you with the assessment of a potential low level technical Privacy breach, a Privacy Breach Checklist has been developed and is provided at Appendix 1.

6. Outcome

If after using the attached Checklist it is determined that it is a *technical (low level)* breach, that is, you answered 'no' to all questions between (a) and (d), and 'yes' to question (e) in Step 2 (ii), then do the following :

- send an email to the notifier acknowledging receipt of the privacy breach and actions taken to remedy breach; and
- create a file/document to record the issue and how it was resolved; and
- send the completed Privacy Breach Notification Form, which includes what remedial has been taken action taken, to RTI and Privacy at privacy@justice.qld.gov.au.

Upon receipt of this information, RTI and Privacy will assess the matter and advise whether any further action is required. The details of the privacy breach will be recorded in RTI and Privacy's CMS database, and included in the weekly report to senior management.

7. Monitor, review and report

The RTI and Privacy team prepares a weekly report for senior management on all privacy breaches, complaints and advices received for the week (including any low level breach notifications). Senior management for the purposes of privacy reporting is:

- Deputy Director-General, Justice Services;
- Assistant Director-General, Strategic Policy and Legal Services;
- Director, Corporate Governance
- Director, Office of the Director-General;
- Corporate Governance; and
- Director, Right to Information and Privacy

Need help or advice?

If you need help or advice with managing these technical (low level) Privacy breaches, please contact from RTI and Privacy on (07) 3738 9893 or email privacy@justice.qld.gov.au.

Appendix 1

Supervisor - Privacy Breach Checklist

The purpose of this Checklist is to provide the DJAG business unit manager, or nominated officer, with a process to follow when assessing a potential technical low level privacy breach.

POTENTIAL PRIVACY BREACH DESCRIPTION

- date and time of the potential technical low level privacy breach?
- date the potential technical low level privacy breach was discovered?
- how was it discovered?
- location of the potential technical low level privacy breach?
- type of personal information involved, for example: residential address; date of birth; medical information; Tax File Number (TFN)?
- format of the information, for example: hardcopy paper; or electronic?
- Is the personal information covered by any confidentiality/non-disclosure provisions in legislation, for example *Youth Justice Act 1992*; *Child Protection Act 1999*; *Working with Children (Risk Management and Screening) Act 2000*?

STEP 1: BREACH CONTAINMENT AND PRELIMINARY ASSESSMENT

- cause of the potential technical low level privacy breach?
- have you contained the technical low level breach?
  - by contacting the individual who received the personal information incorrectly
  - recovered the information, i.e. received advice from the unintended party that the documentation was destroyed or the information has been returned to DJAG
  - by having any on-forwarded copies deleted from IT systems, i.e. Microsoft Office email sent items, inbox and/or deleted items
- if contained and rectified, how long did this take?
- have you determined and informed relevant internal officers who need to be made aware of the incident at this preliminary stage, e.g. supervisor, Assistant Director-General, Deputy Director-General? (Note: if you are unsure of who to advise regarding this briefing process, contact your direct supervisor for advice or RTI and Privacy.)

STEP 2: EVALUATE THE RISKS ASSOCIATED WITH THE BREACH

(i) What personal information was involved?
   a. was the personal information - name, address, financial, medical?
   b. what form was it in - paper records, electronic database?
   c. what physical or technical security measures were in place at the time of the breach - locks, alarm systems, encryption, passwords, TFN, etc?

(ii) What is the extent of the breach?
   a. is there a risk of ongoing breaches or further exposure of the information?
   b. was the information disclosed to a person outside of the business unit, or DJAG?
   c. can the personal information be used for fraudulent or other purposes?
   d. was the information lost or was it stolen? If it was stolen, can it be determined whether the information was the target of the theft or not?
   e. has the personal information been recovered?

STEP 3: NOTIFICATION

Technical (low level) breach – business unit level

If , in Step 2(ii) above, you answered 'no' to all questions (a) to (d), and 'yes' to question (e), the breach is within the low level breach classification then do the following:

- send an email to the notifier acknowledging receipt of the privacy breach and actions taken to remedy breach; and
- create a file/document to record the issue and how it was resolved; and
- send the completed Privacy Breach Notification Form, which includes what remedial has been taken to RTI and Privacy at privacy@justice.qld.gov.au.

Upon receipt of this information, RTI and Privacy will assess the matter and provide advice on the provisions of the IP Act that were technically contravened and advise whether any further action is required. The details of the privacy breach will be recorded in RTI and Privacy's CMS database, and will also be included in RTI and Privacy's weekly report to senior management.

Technical (medium/high level) breach – RTI and Privacy

If, in Step 2(ii) above, you answered 'yes' to any of the questions (a) to (d), or 'no' to question (e) , the breach does not fit under the low level breach classification.

If this is the case, you must immediately complete a Privacy Breach Notification Form, attach all relevant information, including the information the subject of the suspected contravention; copies of any emails or documents involved, details of the officer involved; and names of persons to whom the information has been disclosed, and send it by email to privacy@justice.qld.gov.au.

The details of the privacy breach will be recorded in RTI and Privacy's CMS database; will also be included in RTI and Privacy's weekly report to senior management; and assessment of the privacy breach will be managed by RTI and Privacy. If the breach is determined to be anything other than low level technical, RTI and Privacy will investigate and report on the matter.