

Privacy and Data Breach Policy

V.1.0 – November 2023

Contents

1. Purpose	3
2. Scope	3
3. Key concepts	4
3.1 What is personal information?	4
3.2 What is health information?	5
3.3 When is the identity of an individual apparent or reasonably ascertainable?	5
3.4 What is an incident and a Data Breach?	6
3.5 What is an Eligible Data Breach?	7
3.6 Other definitions	7
4. Policy principles.....	8
4.1 What are the IPPs and HPPs that apply?	8
4.2 Privacy Impact Assessments	10
4.3 Penalties for non-compliance with Information Protection and Health Privacy Principles	11
5. Incidents and Eligible Data Breaches.....	11
5.1 Overview	11
5.2 Preventing Privacy Data Breaches	12
5.3 Reporting and responding to a Data Breach	12
5.3.1 Step 1: Initial report and triage.....	12
5.3.2 Step 2: Contain the breach	13
5.3.3 Step 3: Assess and mitigate	13
5.3.4 Step 4: Notify.....	16
5.3.5 Step 5: Review	19
5.4 Internal Eligible Data Breach Register	20
5.5 Communications Strategy	20
6. Roles and responsibilities	20
7. Related Policies or Procedures.....	21
8. Contact for Enquiries and Feedback.....	22
9. Version Control and Document History.....	23

1. Purpose

This Policy:

- explains how icare collects and manages personal and health information, which it needs to collect for the purposes of exercising its functions and providing services
- serves as icare's Data Breach Policy and sets out how icare will respond to a Data Breach (defined in section 3.4 below), the roles and responsibilities of people working at icare in relation to managing a Data Breach and the steps icare will follow if a breach occurs.

icare needs to collect, access, use and disclose personal or health information as part of its usual business operations and to effectively and efficiently provide services.

icare is committed to protecting the privacy of all individuals whose personal or health information it collects and handles. This Policy sets out the key principles and commitment to action for icare to:

- achieve the goal of ensuring icare responsibly handles and protects all personal information that it collects and possesses
- comply with icare's legal and regulatory obligations as a public sector agency under the *Privacy and Personal Information Protection Act 1998* (the **PPIPA**) and the *Health Records and Information Privacy Act 2002* (the **HRIPA**) and the icare values
- appropriately respond and deal with Data Breaches.

This Policy supports icare's purpose and values. icare's purpose is that we care for the people of NSW, building confidence and trust so our communities can thrive. Further information on icare's purpose and values is available on icare's website at:

<https://www.icare.nsw.gov.au/about-us/our-strategy>

This Policy is supplemented by the icare Privacy Management Plan (**PMP**) which provides further detailed information on how icare collects, uses, discloses and disposes of personal and health information. The PMP is available on icare's website at:

<https://www.icare.nsw.gov.au/privacy>

2. Scope

This Policy applies to:

- everyone working at icare, including directors, all employees (including part-time and temporary employees), graduates, contingent workers, interns, secondees and volunteers
- each claim service provider (**CSP**) and scheme agent who manages claims on behalf of icare

- other service providers that use or hold personal or health information on behalf of icare.

3. Key concepts

3.1 What is personal information?

Personal information is any information or an opinion about an individual, where the identity of that individual is apparent or could reasonably be ascertained from that information or opinion.

Some examples of personal information include:

- a person's name, home address, email and phone number
- a person's date of birth, age, gender, height and weight
- information about a person's personal or family life, such as marital status, religion or beliefs, or sexuality
- a person's signature, user names and passwords
- government identifiers (such as Tax File Numbers)
- identity documents, such as driver's licence details or passport details
- financial information, including bank account details, credit card details or information about a person's wealth and investments
- employment information, including details of salary and personnel records
- information about a person's education and qualifications
- information about a person's membership of voluntary or professional bodies, such as a trade union
- photographs, video or voice recordings of an individual, where that person can be identified
- information about a person's hobbies or interests.

Opinions about an individual also fall within the scope of personal information. Some examples of opinions include:

- a referee's report about a job applicant
- comments made by a supervisor as part of an employee's performance review
- notes that express views about a colleague or a member of the public.

3.2 What is health information?

Health information is personal information or an opinion about any of the following:

- the physical or mental health or disability of an individual
- an individual's express wishes about the future provisions of health services (to that individual)
- health services provided, or to be provided, to that individual.

All personal information collected while providing a health service is also health information (for example, a doctor's clinical notes on a patient).

Health information also includes healthcare identifiers (such as a Medicare number), as well as certain kinds of genetic information about an individual.

Some examples of health information include:

- information about a physical injury, illness, disease or chronic condition suffered by a person
- information about a person's physical disability
- information about a mental health condition or mental illness suffered by a person
- information about any medical treatment received (or to be received) by a person
- an opinion about a person's health, including their future health (for example, a doctor's opinion about a person's likelihood of recovery).

Note that it does not matter whether the relevant health information relates to a past, present or future event.

3.3 When is the identity of an individual apparent or reasonably ascertainable?

A person's identity may be apparent in the information itself. For example, if a person's name is contained in the same record as other information about that person.

A person's identity is reasonably ascertainable if the information could be associated with other information to identify the individual. For example:

- information that is very specific, such that it could not be referring to anyone else – for example, the CEO of Company X
- information can be linked to other information that would permit an individual to be identified – for example, information linked to a person identified only by a serial number may not be personal information. However, if icare also possessed a record linking serial numbers to individuals, then the information will be personal information.

Care should be taken that any data set that is purportedly anonymised or de-identified cannot reasonably be re-identified.

3.4 What is an incident and a Data Breach?

An **incident** is defined in icare's Incident and Issue Management and Reporting Policy, which at the date of this Policy is as follows:

An **incident** is any event which results in an adverse impact on icare, our customers or our people that was caused by:

- a breakdown in processes, controls or systems;
- human error; or
- an external event.

A **Data Breach** occurs when information held by icare (whether held in digital or hard copy) is subject to unauthorised access, unauthorised disclosure or is lost in circumstances where the loss is likely to result in unauthorised access or unauthorised disclosure.

A **Privacy Data Breach** is when the information subject to the Data Breach is personal or health information.

It does not matter if the Data Breach results from an accidental or deliberate act, or if the cause of the event was internal to icare or external.

Some examples of a Privacy Data Breach include:

- an unauthorised third party (such as a hacker) accesses personal or health information held by icare
- personal or health information is unintentionally sent to the wrong recipient (for example, sent to the wrong email address)
- an icare employee who is not permitted to access certain personal or health information, accesses that information (whether deliberately, unintentionally or due to a failure of access controls)
- an icare employee who is only permitted to access certain personal or health information for certain purposes, accesses that information for unauthorised purposes
- a device or document containing personal information is lost (for example, a laptop is accidentally left on the train).

An example of a Data Breach that is not a Privacy Data Breach is when a third party (such as a hacker) gains unauthorised access to a confidential document that contains no personal or health information, such as a confidential technical document regarding icare's IT system.

All Data Breaches, whether or not a Privacy Data Breach, go through the same recording and assessment process (see section 5.3.1 below).

3.5 What is an Eligible Data Breach?

An **Eligible Data Breach** is defined in section 59D of the PPIPA. It is a more serious Data Breach and, briefly stated, occurs where both of the following occur:

- a Privacy Data Breach has occurred (or is likely to have occurred)
- as a result, it is likely that the individual to whom the personal or health information relates would suffer serious harm. Further information on how this “serious harm” assessment must be conducted is set out at section 5.3.3 below.

An Eligible Data Breach also occurs where it cannot be definitively concluded that each of the above conditions have been met, but there are reasonable grounds to suspect that those conditions have occurred.

icare has duties under the PPIPA to respond to Eligible Data Breaches in a particular manner (set out in more detail in section 5 below).

A **Suspected Eligible Data Breach** is a Data Breach that is suspected of being an Eligible Data Breach because from the information currently available an Eligible Data Breach is one of the possible outcomes.

3.6 Other definitions

Authorised Person means any of the following:

- the Chief Executive Officer of icare
- a person delegated by the Chief Executive Officer of icare to exercise the functions of that Chief Executive Officer for the purpose of Part 6A of the PPIPA.¹

Code of Conduct and Ethics Policy means the code of that name available on icare’s website. That code applies to everyone working at icare and provides the guiding principles to support those people in making decisions and choices at their work.

Incident and Crisis Management Plan means the icare plan of that name which guides relevant icare teams on the steps to be undertaken to manage a disruptive event that impacts icare, allowing for effective incident and crisis management, including assessment and triage, escalation and notification, management by the appropriate team and communication.

Incident and Issue Management and Reporting Policy means the icare policy of that name which applies to everyone working at icare and specifies the principles to be adhered to in order to support effective incident and issue management, including identifying, reporting, investigating, responding, reviewing and closing incidents and accountability for them.

¹ Section 59ZJ of the PPIPA

Information and Records Management Policy means the icare policy of that name which outlines the principles to govern how information is created and collected, used and accessed, secured and stored, and retained in accordance with icare's business needs and legal requirements.

Reporting Wrongdoing Policy means the policy of that name available on icare’s website. That policy sets out how icare will support and protect staff, volunteers, contractors and subcontractors that come forward with a report of serious wrongdoing. It further explains how to make that report and how icare will deal with it, protecting those who speak up from detrimental action and making sure icare takes appropriate action to investigate or deal with the report.

4. Policy principles

4.1 What are the IPPs and HPPs that apply?

icare is a public sector agency and is required to comply with the Information Protection Principles and the Health Privacy Principles (together, the “**Principles**”).

icare has regard to the Principles when designing and implementing its services, processes and systems, to ensure that they are built in to icare’s way of doing business.

All icare employees must comply with the Principles when collecting and handling personal or health information.

Summary of relevant Principles

A reference to information in the following table means personal and health information unless specified otherwise.

Title	Summary
Collection	<p>We must only collect information if it is necessary for a purpose that is directly related to icare’s functions and activities.</p> <p>We must make sure that any information we collect is relevant for our purposes, is accurate, up to date and is not unreasonably intrusive.</p> <p>Where practical, we must collect information directly from the person to whom the information relates (or their authorised representative). Where collecting health information from a third party we must take reasonable steps to notify the person that this has occurred.</p> <p>We must provide a Privacy Collection Notice to all individuals at the time that their information is collected, or as soon as practicable after collection. The Privacy Collection Notice must explain what information is being collected, why we are collecting the information, how it will be used, who it will be disclosed to, whether the information is required by law, the consequences of not providing the information, how the information can be accessed and corrected.</p>

Title	Summary
Consent	<p>When relying on consent for use or disclosure of an individual's information, we must ensure that:</p> <ul style="list-style-type: none"> the individual is fully informed of how their information will be used and/or who it will be disclosed to consent is freely given the request for consent is current and specific the individual has capacity to consent.
Retention and Disposal	<p>Information must not be kept for longer than necessary to fulfil the purpose for which it was collected and must be securely disposed of once that purpose is fulfilled. Where information is required to be disposed of, it must be disposed of securely. No document may be disposed of without proper authority.</p> <p>icare (and each scheme managed by icare) is required to comply with the relevant retention and disposal authorities in place and issued by the State Records NSW.</p> <p>Appropriate meta-data must be retained after disposal including information such as the name of the file, the dates of creation and disposal, the disposal authorisation, disposal method etc.</p> <p>Further information is set out in icare's Information and Records Management Policy.</p>
Security	<p>We must protect personal and health information with reasonable and proportional security safeguards against loss and unauthorised access, use, modification or disclosure.</p> <p>We must ensure that appropriate safeguards are in place before personal or health information is given to or accessed by third parties.</p> <p>Further information is set out in icare's Information Security Policy.</p>
Access and correction	<p>We must allow the person to whom the personal and health information relates to access it without excessive delay or expense.</p> <p>We must allow the person to whom the personal and health information relates to update, correct or amend their personal information.</p> <p>Further information is set out on the "Your privacy" page at the following address: https://www.icare.nsw.gov.au/privacy/your-privacy.</p>
Use	<p>We must take steps to ensure that information is relevant, accurate, up to date, complete, not excessive and not unreasonably intrusive before using it.</p> <p>We must only use personal and health information for the purpose it was collected.</p> <p>Generally, consent is needed to use the information for another purpose.</p>

Title	Summary
Disclosure	<p>We must only disclose personal and health information in the following circumstances:</p> <ul style="list-style-type: none"> • the person consented to the disclosure, or • when the information was collected, the person was told that the information would be disclosed and the disclosure relates to the purpose for which the information was collected, or • it is for a directly related purpose to which the information was collected, and the person would expect the disclosure and not unreasonably object to it, or • it is to prevent or lessen a serious or imminent threat to a person's health or safety, or • disclosure of the information is otherwise expressly permitted by law. <p>Sensitive personal information such as ethnic and racial origins, political opinions, religious beliefs cannot be disclosed without consent unless it is to prevent or lessen a serious or imminent threat to a person's health or safety.</p>
Transborder Data Flows	<p>We must have appropriate measures in place to ensure the transfer of personal or health information outside of NSW is done in compliance with legal requirements.</p>
Anonymity, Unique Identifiers and Health Information Linkages	<p>We must allow people to receive services from us anonymously, where it is lawful and practical.</p> <p>In relation to health information, we may only assign unique identifiers (for example, a number) to an individual's health information if it is reasonably necessary to enable us to carry out any of our functions efficiently.</p> <p>We must not include health information in a health records linkage system without the individual's consent.</p>

4.2 Privacy Impact Assessments

When designing and implementing new projects or initiatives that may involve the handling of sensitive or large volumes of personal or health information, the need to conduct a Privacy Impact Assessment (**PIA**) must be considered, including to better enable icare to meet the Principles. Examples of sensitive information in these circumstances will include information relating to an individual's ethnic or racial origin, political opinions, religious or philosophical beliefs, trade union membership or sexual activities.

A PIA provides an opportunity for privacy risks to be avoided or mitigated by ensuring a project complies with the law, meets community expectations, and is as least privacy-invasive and most privacy-enhancing as possible.

A PIA should be conducted at the design stage of a new system or program, and then revisited as program requirements or legal obligations change.

4.3 Penalties for non-compliance with Information Protection and Health Privacy Principles

Breaches of this Policy arising from a deliberate, intentional or negligent act or omission may result in disciplinary action up to and including termination of employment, depending on the circumstances, severity and impact of the breach.

Any instance of non-compliance with this Policy must be managed and reported in accordance with the Incident and Issue Management and Reporting Policy.

To the extent relevant, non-compliance with this and other policies, such as the Code of Conduct and Ethics Policy, could also be reported under icare's Reporting Wrongdoing Policy.

Both the PPIP Act and the HRIP Act contain offences for any person, such as employees, contractors and service providers, who intentionally use or disclose personal information or health information without authority. The maximum penalty for breaching is up to two years' imprisonment and/or an \$11,000 fine. Where relevant, people engaging in such conduct may also be subject to claims for damages and remedies under relevant contracts, such as termination for breach.

If employees are uncertain as to whether certain conduct may breach icare's privacy obligations, they should seek the advice of the Privacy Team.

5. Incidents and Eligible Data Breaches

5.1 Overview

Effective management of incidents and Data Breaches is an essential part of meeting icare's compliance obligations, improving customer experience, and maintaining community trust in how icare deals with people's personal and health information.

Under the PPIPA, certain kinds of Privacy Data Breaches must be notified to the Privacy Commissioner and affected individuals. These are called Eligible Data Breaches. Not all Privacy Data Breaches are Eligible Data Breaches.

This section of this Policy is intended to provide guidance on what to do if a Privacy Data Breach occurs, and when (and how) an Eligible Data Breach is required to be notified to the Privacy Commissioner and affected individuals.

icare has the following measures in place to prepare for a Data Breach:

- annual testing and review of this Policy
- all people working at icare are required to complete annual mandatory privacy training to ensure they know and understand their privacy obligations and how to identify and report a suspected Data Breach
- a privacy awareness strategy to ensure that people working at icare and relevant suppliers are aware of their responsibilities under this Policy

- third-party contracts include, where relevant, provisions for reporting, managing Data Breaches and relevant mandatory training
- post-incident reviews are undertaken to assess icare’s response to the Data Breach and the effectiveness of this Policy.

5.2 Preventing Privacy Data Breaches

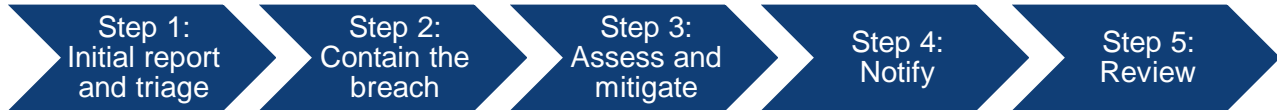
It is within the power of every person working at icare to minimise the risk of a Privacy Data Breach occurring by complying with this Policy, as well as the policies specified in section 7 below, and promptly raising any concerns or issues with their People Leader or Line 1 Risk team.

icare ensures that appropriate safeguards are in place before personal or health information is collected, used by, disclosed to, or accessed by third parties.

Cyber security training and awareness is provided to people working at icare to prevent Data Breaches.

5.3 Reporting and responding to a Data Breach

The five key steps to respond to a Data Breach are as follows:



Each step is set out in further detail below. The first four steps should be carried out concurrently where possible. The last step provides recommendations for longer-term solutions and prevention strategies.

5.3.1 Step 1: Initial report and triage

icare may become aware of a Data Breach by its own employee or by being notified by a customer, service provider or a member of the public.

All suspected or potential Data Breaches must be recorded as an incident in Risk Connect² within two (2) business days of icare becoming aware of it. For privacy incidents, these must be recorded as a “Privacy/Data” incident.

If a person working at icare is unsure if an incident is a suspected or potential Data Breach, they should contact their People Leader or their Line 1 Risk Team for further advice.

² Risk Connect is the name given to icare’s internal governance, risk and compliance system. One use of Risk Connect is to record incidents. Being an internal tool, Risk Connect is not accessible by the public.

Often icare will be unable to determine if a Data Breach is a Privacy Data Breach until after the breach is investigated. Accordingly, if it is unclear that personal or health information is the subject of the Data Breach, then the Data Breach must be recorded as a Privacy Data Breach until determined otherwise.

Members of the public or others outside of icare can report a suspected Data Breach involving personal and/or health information held by icare by emailing the icare Privacy Team at: privacy@icare.nsw.gov.au

Initial investigation

After a Data Breach has been recorded in Risk Connect, the person responsible for managing the incident under the Incident and Issue Management and Reporting Policy (“**Responsible Person**”) must, without delay, investigate and keep records in relation to each Data Breach in accordance with that policy.

The Responsible Person must escalate a Suspected Eligible Data Breach or actual Eligible Data Breach in accordance with section 5.3.3 below.

5.3.2 Step 2: Contain the breach

icare must, without delay, take all reasonable efforts to contain any Data Breach and mitigate the risk of harm to affected individuals.

How a Data Breach is contained will depend on its nature. It may be appropriate to seek the expertise of other icare employees (including IT or Legal) or external service providers (such as, cyber forensics or legal expertise). If the Data Breach involves third party service providers, icare must, without delay, consider what directions it may need to give those providers to help contain and mitigate the Data Breach. The Responsible Person must coordinate the response to the Data Breach (or delegate this responsibility to another icare employee), including with the icare data breach response team relevant in the particular circumstances.

The response may include retrieval and/or deletion of lost data, ceasing unauthorised access, shutting down or isolating affected systems, or consulting with other entities that jointly hold data with icare.

All evidence of the Data Breach should be collected and preserved to allow for the cause of the breach to be determined and to allow measures to be taken to prevent its reoccurrence.

5.3.3 Step 3: Assess and mitigate

After an incident is recorded in Risk Connect it will be promptly evaluated by the Responsible Person and, if assessed as a Suspected Eligible Data Breach, then this must be immediately reported to the Principal Privacy Officer.

Although reporting an incident in Risk Connect applies, a person working at icare may choose to also report a Suspected Eligible Data Breach directly to the Principal Privacy Officer by email, such as when an urgent Suspected Eligible Data Breach occurs.

The Principal Privacy Officer must immediately assess and help mitigate the Suspected Eligible Data Breach, notify the Authorised Person of the Suspected Eligible Data Breach and as soon as practicable, and within 2 business days, provide sufficient information and support to the Authorised Person to help complete the Authorised Person's responsibilities under this Policy and coordinate the relevant data breach response team.

The Authorised Person is responsible for deciding whether an Eligible Data Breach has occurred (or whether there are reasonable grounds to believe an Eligible Data Breach has occurred) and must carry out an assessment on this. The assessment must be carried out in an expeditious way. The Authorised Person may appoint another person(s) to carry out this assessment (an **Assessor**) – however, the Authorised Person remains responsible for deciding whether an Eligible Data Breach has occurred. An Assessor may be another icare employee, an employee of another NSW government agency or an external third party (in each case, provided the person was not otherwise involved in the Data Breach).

In order to assess whether an Eligible Data Breach has occurred, it is necessary to assess whether it is likely that the individual to whom the personal or health information relates would suffer serious harm as a result of the unauthorised access or disclosure.

What is serious harm?

Serious harm includes serious physical, psychological, emotional, financial, or reputational harm.

Examples of serious harm include:

- identity theft – for example, where identity documents have been compromised
- financial loss – for example, where credit card details have been compromised
- physical harm – for example, where a person has an abusive ex-partner and the person's contact details are to be kept secret
- psychological or emotional harm – for example, where sensitive information about a person's health is compromised.

What information must be considered?

The serious harm assessment must be made based on:

- the information that has been accessed or disclosed in the privacy incident
- any other relevant information icare is aware of in respect of the affected individual.

For example, if icare is aware that a person affected by a privacy incident suffers a particular mental illness, then this should be taken into account in the serious harm assessment, even if the information compromised by the privacy incident did not include information about that person's mental illness.

However, icare is not required to seek out further information about the personal circumstances of an affected individual.

What factors must be considered in assessing the likelihood of serious harm?

The following factors must be considered to assess the likelihood of serious harm:³

- the types of personal or health information involved in the privacy incident
- the sensitivity of the personal or health information involved in the privacy incident
- whether the personal or health information is or was protected by security measures
- the persons to whom the unauthorised access to, or unauthorised disclosure of, the personal or health information involved in the privacy incident was, or could be, made or given
- the likelihood of those persons intending to cause harm, or circumventing security measures protecting the information
- the nature of the harm that has occurred or may occur
- any other matter specified in the Privacy Commissioner's guidelines.

An Eligible Data Breach only occurs where serious harm is likely. “Likely” means more probable than not (rather than merely possible).

Additional consideration where personal or health information is lost

In the situation where the incident involves personal or health information being lost (for example, a device accidentally left on the train), the serious harm assessment must also include an assessment of the likelihood that there will be unauthorised access or disclosure of personal or health information.

For example, where a device has both password and two-factor authentication security, and icare’s IT security team is able to remotely wipe the device, it may be possible to conclude that there is a low likelihood that there will be unauthorised access or disclosure of personal or health information on that device, because of that device’s security measures.

Timeframes for determining an Eligible Data Breach

The Authorised Person must decide whether there has been an Eligible Data Breach (or whether there are reasonable grounds to believe an Eligible Data Breach has occurred) within 30 days after an officer or employee of icare becomes aware that there are reasonable grounds to suspect there may have been an Eligible Data Breach for icare. The assessment must be carried out in an expeditious way. The Authorised Person may decide to consult with internal and external expertise or resources to make this decision, although the responsibility remains with the Authorised Person. The Authorised Person must consult with Legal and the Group Executive Risk & Governance before making their decision.

³ Section 59H of PPIPA

Where the Authorised Person has appointed an Assessor, the Assessor must provide their report to the Authorised Person at least 3 business days before the 30 day period ends.

If the Authorised Person believes the assessment cannot be concluded within this 30 day period, then they may extend this by a period reasonably required for the assessment to be concluded. Further extension may also be made. The Authorised Person must consult with Legal and the Group Executive Risk & Governance on any extension, as extensions must be notified to the Privacy Commissioner.⁴

5.3.4 Step 4: Notify

If the Authorised Person decides that an Eligible Data Breach has occurred (or there are reasonable grounds to believe an Eligible Data Breach has occurred), then the notification process is triggered. There are four elements of the notification process:

1. Notify the Privacy Commissioner immediately after an Eligible Data Breach is identified using the approved form
2. Determine if any of the six exemptions for notifying an Eligible Data Beach apply⁵ and icare is not required to notify affected individuals
3. Notify individuals: Unless an exemption applies, notify affected individuals or their authorised representative as soon as practicable (see “When to notify” below)
4. Provide further information to the Privacy Commissioner as required.

icare recognises that notification to individuals or organisations affected by a Data Breach can assist in mitigating any damage for those affected. Notification demonstrates a commitment to open and transparent governance, consistent with icare’s values.

If a Data Breach is not an Eligible Data Breach, icare may still consider notifying individuals and organisations of the breach dependent upon the type of information that is involved, the risk of harm, repeated and/or systematic issues and the ability of the individual to take further steps to avoid or remedy harm.

Notification should be undertaken promptly to help avoid or lessen the damage by enabling the individual and/or organisation to take steps to protect themselves. The PPIPA requires icare to take reasonable steps to notify affected individuals of an Eligible Data Breach as soon as practicable (see “When to notify” below).

The method of notifying affected individuals and organisations will depend in large part on the type and scale of the breach, as well as immediately practical issues such as having contact details for the affected individuals and organisations. Some of the considerations are set out below.

⁴ Section 59K of the PPIPA

⁵ Part 6A Div 4 of the PPIPA

Notification to the Treasury Managed Fund

The Treasury Managed Fund (TMF) is a self-insurance scheme created by the NSW government to cover NSW government agency risk. The TMF indemnifies icare for most insurable risks, including liability for claims due to most Data Breaches and non-compliance with privacy legislation.

The Authorised Person will notify the TMF of any potential claims or liability (as per the TMF Statement of Cover).

When to notify

The PPIPA requires icare to take reasonable steps to notify affected individuals of an Eligible Data Breach as soon as practicable. What being notified as soon as practicable means will depend on the circumstances, but typically means notifying when notice is capable of being put into practice with the available means.

The Privacy Commissioner's guidelines highlight that:

- timely notification is important to help individuals affected by a breach take steps to limit or mitigate the risks of misuse or further exposure
- icare should avoid undue delay and work to make affected individuals aware of the breach as soon as possible
- icare should carefully balance speedy notification to individuals with ensuring that people are provided with reliable and accurate information about the breach
- notifications should provide recipients with an accurate sense of what risks may arise for them and what practical measures they can take to protect themselves. An inaccurate notification could cause more harm than good, such as unnecessary anxiety and fail to enable those affected to take protective action. If icare is not yet able to provide meaningful detail in a notification, it may be too early to provide it
- for complex breaches or where significant numbers of individuals are affected, icare may need to consider a triage system to notification, such as notifying in tranches based on the level of risk posed to the individual or the sensitivity of the information involved in the data breach.

Where individuals affected by an Eligible Data Breach cannot be notified, icare will consider issuing a public notification on our website (see "How to notify" below).

How to notify

Generally, affected individuals and organisations should be notified directly (by telephone, letter, email or in person).

In some circumstances, it may not be practical for icare to notify affected individuals directly. For example, where the contact information of affected individuals and organisations is unknown, or where direct notification is prohibitively expensive or could cause further harm (for example, by alerting a person who stole the laptop as to the value of the information contained). When this occurs, icare may consider a public notification (such as information

icare's website, a public notice in a newspaper, or a media release). A record of any public notification of an Eligible Data Breach will be published on icare's website and recorded on the Public Data Breach Notification Register for a period of at least twelve months.

What to say

The PPIPA sets out the information that must be included in notifications to individuals, including:

- the date the breach occurred
- a description of the breach
- how the breach occurred
- the type of breach that occurred
- the personal information included in the breach
- the amount of time the personal information was disclosed for
- actions that have been taken or are planned to secure the information, or to control and mitigate the harm
- recommendations about the steps an individual should take in response to the breach information about complaints and reviews of agency conduct
- the name of the agencies that were subject to the breach
- contact details for further information about the breach.

Other notification obligations

The Authorised Person will also consider whether other organisations, agencies or regulatory bodies should be notified of a Data Breach (whether or not it is an Eligible Data Breach). Depending on the circumstances this could include:

- NSW Police Force and/or Australian Federal Police, where icare suspects a Data Breach is a result of criminal activity
- Cyber Security NSW, the Office of the Government Chief Information Security Officer and The Australian Cyber Security Centre, where a Data Breach is a result of a cyber security incident
- The Office of the Australian Information Commissioner, where there are notification requirements under the *Privacy Act 1988*
- Any third-party organisations or agencies whose data may be affected
- Financial services providers, where a Data Breach includes an individual's financial information
- Professional associations, regulatory bodies or insurers, where a Data Breach may have an impact on these organisations, their functions and their clients
- The Australian Cyber Security Centre where a Data Breach involves malicious activity from a person or organisation based outside Australia.

The Authorised Person must consult with Legal and the Group Executive Risk & Governance before making any of the above notifications.

Incidents assessed as not being an Eligible Data Breach

If the Authorised Person determines that an Eligible Data Breach has not occurred, then icare is not required by the PPIPA to notify either the Privacy Commissioner or affected individuals about the Data Breach.

In this situation, the Authorised Person should decide whether the Privacy Commissioner or affected individuals should be notified on a voluntary basis. The Authorised Person must consult with Legal and the Group Executive Risk & Governance before making any notification on a voluntary basis.

Voluntary notification of individuals should only be made in exceptional circumstances, such as when the benefits of voluntary notification materially outweigh the potential harm. This is because notifying individuals about a Data Breach that poses very little or no risk of serious harm can cause unnecessary anxiety and inconvenience. If icare notifies individuals of Data Breaches when not required to do so under the PPIPA, then this could lead to people being de-sensitised to these kinds of notices, so they don't take a notification seriously, even when there is a real risk of serious harm. These factors should be taken into account when deciding whether to notify individuals on a voluntary basis.

5.3.5 Step 5: Review

After a Data Breach has been resolved, it may be necessary to conduct a review to assess how it occurred, and what changes may be made to prevent reoccurrence.

This should include a review and remediation of:

- the internal controls in place
- policies and procedures
- staff skills and training
- contractual obligations with contracted service providers
- any other material issues relevant to the Data Breach.

A post-incident review, including an assessment of how icare responded to the Data Breach, must be carried out:

- for Eligible Data Breaches
- where a Privacy Data Breach arose as a result of a malicious act
- where systemic shortcomings in icare's processes or systems have been identified
- in any other situation as determined by the Group Executive Risk & Governance.

If a post-incident review raises any issues or concerns about the effectiveness of this Policy, this should be reported to the Group Executive Risk & Governance.

5.4 Internal Eligible Data Breach Register

All Eligible Data Breaches must be recorded on icare’s internal Data Breach Incident Register as soon as practicable by the Privacy Team and within 2 business days. The Principal Privacy Officer is responsible for ensuring that the register is up to date and accurate.

5.5 Communications Strategy

Depending on the nature and/or scale of the Eligible Data Breach, a communications strategy may need to be implemented by icare. icare’s Incident and Crisis Management Plan contains roles and responsibilities for managing communications when an incident occurs.

6. Roles and responsibilities

Role	Responsibilities
All Employees	<ul style="list-style-type: none"> Always comply with the requirements of this Policy. Actively consider privacy risk in business processes and related activity, take action to mitigate or escalate issues if necessary. Implement and/or support the implementation of controls to mitigate privacy risk. Complete mandatory privacy awareness and related training. Report and/or escalate privacy incidents, ‘near misses’ and issues in Risk Connect in accordance with this Policy. Initiate and maintain appropriate records.
Authorised Person	<ul style="list-style-type: none"> Assess whether privacy incidents are Eligible Data Breaches and fulfil the role of Chief Executive Officer of icare under Part 6A of the PPIPA. Supervise communication with the NSW Privacy Commissioner and the Office of the Australian Information Commissioner in relation to Data Breaches. Notify Eligible Data Breaches to the NSW Information Privacy Commissioner or the OAIC as required.
Board	<ul style="list-style-type: none"> Review and approve this Policy annually. Set the tone at the top for the culture and objectives of this Policy within icare. Accountable for the effectiveness of this Policy and its application.
Board Risk Committee	<ul style="list-style-type: none"> Oversee the effective implementation of this Policy and icare’s approach to privacy management. Ensure that icare has adequate resources and effective arrangements for privacy management. Review and endorse this Policy prior to Board approval.
Group Executive – Risk & Governance (in addition to above)	<ul style="list-style-type: none"> Oversee the regular review of this Policy and icare’s Privacy Management Plan and recommend changes and updates for approval by the Board as appropriate. Report to senior management and the icare Board Risk Committee on privacy issues and incidents and the overall management of privacy risk across icare.

Role	Responsibilities
Group Executives	<ul style="list-style-type: none"> • Drive a culture of compliance with this Policy and raise awareness of robust and pro-active privacy management practices. • Accountable for implementing this Policy, managing privacy risk, remediation of privacy incidents and the ongoing adherence to the Policy within their businesses. • Ensure all people working in their business unit have completed all privacy training and understand their privacy obligations.
Legal	<ul style="list-style-type: none"> • When requested, provide legal advice on matters relevant to this Policy and icare’s activities under it, such as changes to relevant legislation and advice on serious harm and Eligible Data Breach.
Line 1 Risk	<ul style="list-style-type: none"> • Support the business in complying with this Policy, including promoting an understanding of privacy obligations, identifying privacy risk and implementing management controls. • Provide support and advice to the business in managing privacy risks, issues and incidents.
Line 2 Risk and Compliance	<ul style="list-style-type: none"> • Monitoring of privacy risk and the operation of the privacy management program across icare • Provide support, challenge and advice to the business in managing privacy risks, issues and incidents
Principal Privacy Officer	<ul style="list-style-type: none"> • Develop icare’s statutory Privacy Management Plan for approval by the Group Executive Risk & Governance. • Monitor legislative and regulatory changes which may impact the way icare processes and manages personal information and advise icare on its application. • Monitor the currency and effectiveness of this Policy and compliance with it and support the Group Executive Risk & Governance with reporting to icare governance committees. • Provide guidance and advice on the development of processes and procedures for management of privacy • Establish the requirements for completing privacy impact assessments. • Develop training and awareness for privacy related policies and procedures. • Provide advice on privacy queries, issues and incidents escalated from Line 1 Risk and Compliance. • Respond to and manage information access requests under the PPIPA and HRIPA, escalated privacy complaints and Privacy Internal Review applications.

7. Related Policies or Procedures

This Policy should be read in conjunction with the Privacy Management Plan and the following policies:

- Code of Conduct and Ethics Policy
- Incident and Crisis Management Plan
- Incident and Issue Management and Reporting Policy
- Information and Records Management Policy
- Reporting Wrongdoing Policy

8. Contact for Enquiries and Feedback

The icare Privacy Team are the best people to speak with for icare personnel who have any questions or feedback. They can be contacted by emailing privacy@icare.nsw.gov.au.

9. Version Control and Document History

Document Name & Version	Privacy and Data Breach Policy V1.0
Document owner	Group Executive Risk & Governance
Approving Authority	Board
Last Approval Date	27 November 2023
Review Frequency	Annually

Version	Author	Change Summary	Approval Date
v1.0	Principal Privacy Officer	Updated policy to comply with amendments under the <i>Privacy and Personal Information Protection Act 1998</i> (NSW).	27 November 2023