PENRITH CITY COUNCIL

POLICY DOCUMENT

POLICY NAME
Privacy Management Plan

DATE ADOPTED
28 November 2023

REVIEW DATE
31 March 2025

COUNCIL MINUTE NUMBER
Not Applicable

RELATED DOCUMENTS
GIPA Policy
Information Guide
Data Breach Policy

RESPONSIBLE DEPARTMENT
Legal Services

POLICY TYPE
Organisational – adopted by General Manager

Document Control

Policy History	Date
Version 1 adopted by the General Manager, Warwick Winn 	**20 May 2021**
Version 2 adopted by the General Manager, Andrew Moore 	**28 November 2023**

Contents

INTRODUCTION

Penrith City Council respects the privacy of its residents, ratepayers, employees and the people who use its services, and has adopted this Privacy Management Plan ("PMP"). The purpose of the PMP is to ensure compliance with the Privacy and Personal Information Protection Act 1998 ("PPIPA"), the Government Information (Public Access) Act 2009 ("GIPA

Act") and the Health Privacy Principles under the Health Records and Information Privacy Act 2002 ("HRIPA"). The PMP is also in place to ensure that the privacy of individuals is respected through the appropriate management and protection of personal and health information held by Council.

This PMP aims to provide a framework to direct strategies and practices which will enable compliance with our legal obligations in relation to the collection, use, management and storage of personal and health information. This document works with other Council guidelines and policies including the Code of Conduct and Rights to Access Information.

Whilst Penrith Council is subject to the PPIP Act, this has been modified by the Privacy Code of Practice for Local Government ('the Code'). Where there have been modifications, this shall be outlined within this plan.

This Plan also outlines how Council will incorporate the 12 Information Protection principles into our everyday functions.

Council collects, stores and uses a broad range of information. A significant part of that information is personal information. This Plan applies to that part of the Council's information that is personal information.

PART 1 – PERSONAL INFORMATION

1.1 Application of this Plan

The PPIPA, the HRIPA and this Plan apply, wherever practicable, to:

- Councillors
- Council employees
- Consultants and contractors of the Council
- Council committees (including community members of those committees which may be established under s355 of the Local Government Act (LGA)).

Council will ensure that all such parties are made aware that they must comply with the PPIPA, the HRIPA, and any other applicable Statutory Guideline, Privacy Code of Practice and this Plan.

1.2 What Is 'Personal Information' And 'Health Information?

'Personal information' is defined by s4 of the PPIPA and is classed as 'information or an opinion about an individual whose identity is apparent or can reasonably be ascertained from the information or opinion. This information can be on a database and does not necessarily have to be recorded in a material form.'

Health information is personal information about the physical or mental health or a disability of an individual, or a health service provided or to be provided to an individual.

Some personal and health information is excluded from provisions of the Acts including information about a person who has been dead for 30 years or longer, and information about a person's suitability for appointment or employment as a public sector official. Information of the latter kind will continue to be handled by Council in an appropriately sensitive manner.

1.3 What is not 'Personal Information'?

'Personal information' does not include 'information about an individual that is contained in a publicly available publication'. Personal information, once it is contained in a publicly available publication, ceases to be covered by the PPIPA.

Section 4A of the PPIPA specifically excludes 'health information', as defined by s6 of the HRIPA, from the definition of 'personal information', but includes 'health information' in the PPIPA's consideration of public registers (discussed below).

Where the Council is requested to provide access or make a disclosure and that information has already been published, then the Council will rely on the provisions of the relevant Act that authorises Council to hold that information and not the PPIPA (for example, s8 of the GIPA Act).

Council considers the following to be publicly available publications:

- An advertisement containing personal information in a local, city or national newspaper
- Personal information on the internet
- Books or magazines that are printed and distributed broadly to the general public
- Council Business papers are available to the general public
- Personal information that may be a part of a public display on view to the general public.

Information published in this way ceases to be covered by the PPIPA.

Council's decision to publish in this way must be in accordance with the PPIPA.

1.4 Personal Information held by Council

The Council holds personal information concerning Councillors, such as:

- Personal contact information
- Complaints and disciplinary matters
- Pecuniary interest returns
- Entitlements to fees, expenses and facilities.

The Council holds personal information concerning its customers, ratepayers and residents, such as, but not limited to:

- Names and home addresses of individuals
- Property ownership and rates records
- Information contained in DA applications and submissions
- Community service utilisation
- Library lending records
- Burial and cremation records
- Applications for various approvals such as the removal or trimming of trees
- Service requests or complaints
- Information concerning children attending child care centres and their families
- Information related to law enforcement activities
- Biographical information held for the purpose of citation in speeches, awards or other forms of recognition
- CCTV footage
- Webcasting and audio recordings

- Donation, grant and sponsorship applications.

Council holds health information including information about the health status of:

- Some residents and ratepayers, where the information is acquired while carrying out Council functions
- Children attending day care centres
- Customers using and attending fitness and health services located in Council's recreation facilities.

1.5 Applying to prevent disclosure of Personal Information

Any information that is removed from, or not placed on, that aspect of a public register to be made public may be kept on the register for other purposes. That is, the information may still be used for Council functions, but it cannot be disclosed to other parties.

An application for suppression should be made in writing addressed to the General Manager and must outline the reasons for the request. The Council may require supporting documentation where appropriate.

Further, under section 739 of the LGA, a person can make an application to suppress certain material that is available for public inspection in circumstances where the material discloses or would disclose the person's place of living if the person considers that the disclosure would place the personal safety of the person or their family at risk.

Section 739 of the LGA relates to publicly available material other than public registers. As such, it limits disclosure in those circumstances where an application for suppression is successful. An application for suppression must be verified by statutory declaration and otherwise meet the requirements of section 739. When in doubt, Council will err in favour of suppression.

1.6 Unsolicited Information

Unsolicited information is personal or health information received by Council in circumstances where Council has not asked for or required the information to be provided.

This information is not subject to the collection principles in the PPIPA or HRIPA but the storage, use and disclosure principles will apply to any record of such information retained by Council.

1.7 Webcasting or Audio Recording

Personal or health information disclosed publicly and recorded for the purposes of webcasting at Council Meetings or Audio Recording at meetings is not deemed to have been collected by Council. Retention and use principles of this information will apply to such information in Council's possession, however disclosure principles will not apply as the information was voluntarily disclosed with the prior knowledge that it would be recorded, broadcast via the internet to the public and made available by Council for public viewing or hearing.

PART 2 – PUBLIC REGISTERS

A public register is a register required by law to be available for public inspection or which Council chooses to make available for public inspection (s3 of the PPIPA).

Disclosure in relation to public registers must comply with Part 6 of the PPIPA and the Privacy Code. Personal information cannot be accessed by a person about another person unless the

personal information is contained in a public register. Where personal information is contained in a public register, then Part 6 of the PPIPA applies to determine whether access to that information will be given to another person.

Disclosure in relation to all other personal information must comply with the Information Protection Principles as outlined in Part 3 of this Plan and the Privacy Code where it includes personal information that is not published.

Members of the public may enquire only in accordance with the primary purpose of any of these registers.

The primary purpose for each of these public registers is set out in the sections that follow.

2.1 Public Registers, the PPIPA and the HRIPA

Council is required by law to maintain a number of public registers and to make them available for public inspection. Some of these registers contain personal information as defined in the Acts.

Despite the exclusion of 'health information' from the definition of 'personal information' under s4A of the PPIPA, section 56A of the PPIPA includes as 'personal information', 'health information' on public registers.

Any person may inspect a public register at a Council office and copy an entry or page but s57 of the PPIPA imposes very stringent controls over the disclosure of personal information contained in a public register. It provides broadly that where Council is responsible for keeping a public register, it will not disclose any personal information kept in that register unless it is satisfied that the information is to be used for a purpose relating to the purpose of the register or the Act under which the register is kept. Council reserves the right to require a person seeking access to provide information about the purpose for which the information will be used (and may require a supporting statutory declaration (s57(2) of PPIPA). Please see further information under the Council's access to information page.

If the stated purpose of the applicant does not conform with the purpose for which the public register is kept, access to the information sought will not be given.

However, the Privacy Code of Practice for Local Government modifies Council's responsibilities concerning public registers in the following way:

- Council should not require a person to provide a reason for inspecting Council's pecuniary interest register or any other register in which Council records declarations made by Councillors or designated officers under *Chapter 14* Part 2 Divisions 3 or 4 of the LGA. However, s.5 of the PPIPA provides that nothing in it affects the operation of the GIPA. S.55(1) of the GIPA allows an assessing officer to consider the motives of a person in seeking access to any document, including the pecuniary interest register (Note: the PPIPA and the Privacy Code of Practice for Local Government pre-date the GIPA).

- Council may provide access to the whole or substantial part of a public register if names and addresses are removed or Council is satisfied that the person requesting the information is to be used for the purpose for which the register is kept, for example, for building certificates, s.6.26 of the Environmental Planning and Assessment Act 1979 (EPA Act) must be complied with.

Where personal information is contained in a publicly available publication, that information will not be regarded as personal information covered by the PPIPA or as health information for the purposes of part 6 of the PPIPA.

2.2 How does this affect the GIPA Act?

Council can only disclose personal information in a public register under the GIPA Act if it also complies with PPIPA.[1] Therefore:

1. If a register is listed in Schedule 1 of the GIPA Regulation, access must not be given except if it is used for a purpose relating to the purpose of the register or the Act under which the register is kept (s57(1) PPIPA)

2. If a register is not listed in Schedule 1 of the GIPA Regulation, access must not be given except:

   (i) If it is allowed under section 57(1) of the PPIPA; and

   (ii) There is no overriding public interest against disclosure of the information under s6 of the GIPA Act.

   Note: Both 1 and 2 are amended with regard to specific public registers in the Privacy Code of Practice for Local Government, as noted in 2.1.

2.3 Where some information in the Public Register has been Published

The part of a public register that is not published in a publicly available publication will be treated as a 'public register' and the following procedure for disclosure will apply.

For example, the Register of Consents and Approvals held by Council under s4.58 of the EPA Act requires Council to advertise or publish applications for development consent.

When Council publishes the address of the property, it may identify the owner. The personal information that has not been published, such as any applications not advertised or that have been rejected or withdrawn (and hence also not published), will be treated as a public register under PPIPA.

A public register must not disclose any personal information kept in the register unless Council is satisfied that it is to be used for a purpose relating to the purpose of the register or the Act under which the register is kept.

2.4 Disclosure of Personal Information Contained in the Public Registers

A person seeking a disclosure concerning someone else's personal information from a public register must satisfy Council that the intended use of the information is for a purpose (see 2.5) relating to the purpose of the register or the Act under which the register is kept. They must make a specific application to Council and outline their reasons and purpose.

2.5 Purposes of Public Registers

2.5.1 Purposes of Public Registers Under the Local Government Act

Land Register – The primary purpose is to identify all land vested in Council, or under its control. The secondary purpose includes a consideration of public accountability as to the land held by Council. Third party access is therefore a secondary purpose.

[1] *Section 57 of the PPIPA prevails over clause 1(3) of Schedule 1 of the Government Information (Public Access) Regulation 2009 (GIPA Regulation) to the extent of any inconsistency.*

Records of Approvals – The primary purpose is to identify all approvals granted under the LGA.

Register of Pecuniary Interests – Whilst the primary purpose of this register is to determine whether or not a Councillor or a member of a Council committee has a pecuniary interest in any matter with which the Council is likely to be concerned, the Privacy Code of Practice for Local Government notes that Councils should not ask for reasons when requests to access this register are made, however, s.5 of the PPIPA provides that nothing in it affects the operation of the GIPA Act. S.55(1) of the GIPA Act allows an assessing officer to consider the motives of a person in seeking access to any document, including the pecuniary interest register.

Rates Record – The primary purpose is to record the value of a parcel of land and record rate liability in respect of that land. The secondary purpose includes recording the owner or lessee of each parcel of land. For example, that a disclosure on a s603 (of the LGA) rating certificate that a previous owner was a pensioner is considered to be allowed, because the secondary purpose is 'a purpose relating to the purpose of the register'. Further, a person may seek access to the owner's details of the neighbouring property for the purposes of a dividing fence, by the completion of a statutory declaration.

2.5.2 Purposes of Public Registers Under the Environmental Planning and Assessment Act

Register of consents and approvals – The primary purpose is to identify applications for development consent and other approvals, confirm determinations on appeal and identify applications for complying development certificates.

Record of building certificates – The primary purpose is to identify all building certificates.

2.5.3 Purposes of Public Registers Under the Protection Of the Environment (Operations) Act

Public register of licences held – The primary purpose is to identify all licences granted under the Act.

2.5.4 Purposes of The Public Register Under the Impounding Act

Record of impounding – The primary purpose is to identify any impounding action by Council.

2.5.6 Other Purposes

Council will allow a person to access their own personal information in a public register to confirm those details if the person can prove their identity to Council.

Persons or organisations who apply to Council to have access to the information contained in any public register for a purpose not related to the purpose of the register, may be given access at the discretion of Council but only in accordance with the Privacy Code of Practice for Local Government concerning Public Registers.

Among the public registers that Council holds and may contain personal information are as follows:

- Delegations register
- Register of Burials

- Records of Approvals
- Land Register
- Register of Consents and Certificates regarding development applications including Complying Development Certificates and Building Certificates
- Register of Licences under the Protection of the Environment (Operations) Act
- Register of Contributions imposed by Council in connection with approval of development
- Record of Impounding under the Impounding Act 1993
- Contracts Register
- Register of Pecuniary Interests
- Disclosures Log under the GIPA Act
- Rates Record.

2.6 Suppression of Information

A person about whom personal information is contained (or proposed to be contained) in a public register, may request Council under s58 of the PPIPA to have the information removed from, or not placed on the register.

If Council is satisfied that the safety or wellbeing of any person would be affected by not suppressing the personal information as requested, Council will suppress the information in accordance with the request unless Council is of the opinion that the public interest in maintaining public access to the information outweighs any individual interest in suppressing information, in accordance with s58(2) of the PPIPA.

2.7 Applications for Access to Own Records on a Public Register

A person wishing to have access to a public register to confirm their own details needs only to prove their identity to Council before having access to their own personal information.

2.8 Other Registers

Council may have other registers that are not public registers. The Information Protection Principles, this Plan, any applicable Codes and the PPIPA apply to those registers or databases.

PART 3 – THE INFORMATION PROTECTION PRINCIPLES

3.1 Collection of Personal Information for Lawful Purposes – Information Protection Principle 1

Council will only collect personal information for a lawful purpose as a part of its proper functions.

Council will not collect personal or health information by any unlawful means.

Council will not collect any more personal information than is reasonably necessary for it to fulfil its proper functions.

Anyone engaged by Council as a private contractor or consultant that involves the collection of personal information must agree to be bound not to collect personal information by any unlawful means. This will include debt recovery actions by or undertaken on behalf of Council by commercial agents.

Companion Animals Act

Collection of information under the Companion Animals Act and Council's use of the Companion Animals Register should be guided by the Director General's guidelines, which have been developed with the PPIPA in mind.

3.2 Direct Collection - Information Protection Principle 2

Council will usually collect information directly from the individual concerned but may collect from others where:

- The individual has authorised collection from someone else, for example in nominating referees when applying for a position with Council
- In the case of personal information relating to a person who is under the age of 16 years, information is collected from a parent or guardian, or with regard to health information about a child under 18 years of age, from the person having parental responsibility
- Indirect collection is necessary in Council's conduct of a lawful investigation or the capacity to detrimentally effect a Council's investigation or complaint handling mechanism
- Information is provided to Council in accordance with legislative requirements or the collection is undertaken as required by another Act, for example, information provided to Council by the NSW Government Land and Property Information Service about transfers of property and associated matters is provided under the LGA
- Information is collected in connection with proceedings before a court or tribunal
- It is unreasonable or impracticable in the circumstances to collect health information directly from the individual
- The collection of personal information indirectly is permitted under the Privacy Code of Practice for Local Government or the Code of Conduct.

Council is also required by law to undertake pre-employment screening, including collection of information for people working with children.

Council will seek to contractually bind each of these bodies or persons to comply with the PPIPA.

Where Council consultants, contractors or committees collect personal information on behalf of Council or in relation to the performance of their activities, that body or person will be required to:

- Obtain a written or electronic authorisation and consent to that collection; and
- Notify those persons in accordance with Information Protection Principle 3 as to the intended recipients and other matters required by that principle.

Committees, private contractors or consultants must abide by this Plan, the Code and the PPIPA under the terms of their incorporation by Council or by contract.

3.3 Requirements when collecting Personal Information - Information Privacy Principle 3

When Council collects personal information from an individual, we will take all steps as are reasonable in the circumstances to ensure that the individual is made aware of the following:

a) The fact that the information is being collected
b) The purposes for which the information is being collected
c) The intended recipients of the information
d) Whether the supply of the information by the individual is required by law or is voluntary, and any consequences for the individual if the information (or any part of it) is not provided
e) The existence of the right of access to, and correction of, the information,
f) Council's name and address, as the agency collecting and holding the information.

Council will ensure that relevant forms and applications include a statement that addresses these matters.

Rights of access are as set out in this Plan.

Council will ensure that any collection of personal information by use of security video cameras or other devices will be accompanied by appropriate signage as required by law.

Staff have been provided with notice regarding surveillance in accordance with the NSW Workplace Surveillance Act 2005.

Council is not required to give notice of collection where:

- The information is unsolicited or has been lawfully collected from someone other than the person concerned
- The person consents to dispensing with the requirement
- Collection is reasonably necessary to confer an award, prize or benefit or similar form of personal recognition on the person (Privacy Code of Practice for Local Government)
- Collection is necessary in Council's conduct of a lawful investigation
- Information is collected in connection with proceedings before a court or tribunal
- Compliance would prejudice the interests of the individual to whom the information relates.

3.4 Other requirements relating to collection of Personal Information - Information Protection Principle 4

When Council collects personal or health information from an individual, it will take such steps as are reasonable to ensure that the information collected is relevant to that purpose, is not excessive and is accurate, up to date and complete, and the collection of the information does not intrude to an unreasonable extent on the personal affairs of the individual to whom the information relates. Council will in normal circumstances rely on the provider of the information regarding accuracy and completeness, although in special circumstances some verification processes may be necessary or appropriate.

3.5 Retention and Security of Personal Information - Information Protection Principle 5

Council will ensure that:

(a) Information is kept for no longer than is necessary for the purposes for which the information may lawfully be used, and
(b) That the information is disposed of securely and in accordance with any requirements for the retention and disposal of personal information, and
(c) That the information is protected, by taking such security safeguards as are reasonable in the circumstances, against loss, unauthorised access, use, modification or disclosure, and against all other misuse, and
(d) That, if it is necessary for the information to be given to a person in connection with the provision of a service of Council, everything reasonably within the power of the Council is done to prevent unauthorised use or disclosure of the information.

3.6 Information Held - Information Protection Principle 6

Council takes reasonable steps to enable a person to determine whether the Council holds personal information about them. If Council holds any information about a person, upon request, it will advise them of the nature of that information, the main purposes for which it is held, and that person's entitlement to access. As a matter of practicality, not every item of personal information, however insignificant, will be capable of being accessed.

Pursuant to s20(5) of the PPIPA, the provisions of the GIPA Act that impose conditions or limitations (however expressed) with respect to any matter referred to in IPPs 6,7 or 8 are not affected by the PPIPA, and those provisions (the ones in the GIPA Act) continue to apply in relation to any such matter as if those provisions were part of the PPIPA. In other words, Council must consider the relevant provisions of the GIPA Act.

Any person can make application to Council by completing the appropriate form and submitting it to Council.

Where Council receives an application or request by a person as to whether Council holds information about them, Council will undertake a search of its records to answer the enquiry. Council may ask the applicant to describe what dealings the applicant has had with Council in order to assist Council to conduct the search.

Council will ordinarily provide a response to applications of this kind within 28 days of the application being made. The fee structure is commensurate to that of the Council's GIPA Act rates structure.

Council is exempt from complying under s25(a) and (b) of PPIPA, where we are lawfully authorised or required not to comply, or where it is 'necessarily implied' or 'reasonably contemplated' under Act or law.

The Council will include a privacy statement to be included on our website concerning the type of personal information we regularly collect, the purpose for which the personal information is used and an individual's right to access their own personal information.

3.7 Access to Personal Information - Information Privacy Principle 7

If Council holds personal information it must, at the request of the individual to whom the information relates and without excessive delay or expense, provide the individual with access to the information.

S14 of the PPIPA requires a Council, at the request of any person, to give access to that person to personal information held about them.

Compliance with this does not mean a person is allowed access to information about other people. If access to information that relates to someone else is sought, the application must be made under the GIPA Act, unless IPPs 11 and 12 or the Public Register provisions apply.

Where a person makes an application for access under the PPIPA and it is involved or complex, it may be referred with the written consent of the applicant as an application under the GIPA Act. The applicant has the right to insist on being dealt with under PPIPA.

Under s20(5) of the PPIPA, IPP 7 is subject to any applicable conditions or limitations contained in the GIPA Act. Council must consider the relevant provisions of the GIPA Act.

Customers wishing to exercise their right of access to their own personal information should apply in writing or direct their enquiries to the General Manager, who will make a determination. An application form may be accessed on Council's website.

In order to comply with the requirement to provide the requested information "without excessive delay or expense", Council will ordinarily provide a response to applications of this kind within 28 days of the application being made.

Council is exempt from complying under ss25(a) and (b) of PPIPA, where we are lawfully authorised or required not to comply, or where it is 'necessarily implied' or 'reasonably contemplated' under Act or law.

3.8 Alteration of Personal Information - Information Protection Principle 8

S15 of the PPIPA allows a person to make an application to Council to amend (this includes by way of corrections, deletions or additions) personal information held about them so as to ensure the information is accurate, and, having regard to the purpose for which the information is collected, relevant to that purpose, up to date and not misleading.

The request should be accompanied by appropriate evidence as to the strength of making the amendment, sufficient to satisfy the Council that the proposed amendment is factually correct and appropriate. The Council may require further documentary evidence to support certain amendments.

Council wishes to have its information current, accurate and complete. Proposed amendments or changes to the personal information held by the Council are welcomed.

If Council declines to amend personal information as requested, it will on request of the individual concerned place an addendum on the information in accordance with section 15(2) of the PPIPA.

Any alterations that are or could be the subject of a customer complaint or grievance will be referred to the Public Officer, who will make a determination in relation to the matter.

Council may refuse to amend information where it is not satisfied that it is incorrect or incomplete. If Council refuses a request for amendment, the individual may request a notation be added to the record.

If information in a Council record is amended, the person is entitled, if practicable, to have previous recipients of that information notified of the amendments.

3.8.1 Existing exemptions under the Act

Compliance with IPP 8 is also subject to certain exemptions under the Act. If one of those

exemptions apply, Council need not comply. The statutory exemption will be relied upon only in limited circumstances and legal advice should normally be obtained.

Council is exempt from complying under s25(a) and (b) of PPIPA, where we are lawfully authorised or required not to comply, or where it is 'necessarily implied' or 'reasonably contemplated' under Act or law.

The Council's application form for alteration is accessible on Council's website.

3.9 Accuracy Of Personal Information before use - Information Protection Principle 9

Prior to use or disclosure Council will take steps reasonable in the circumstances to ensure that information is relevant, accurate, up to date, complete and not misleading.

3.10 Use of Personal Information - Information Protection Principle 10

Use means the employment of information for a purpose associated with Council functions. Council will not use personal information for a purpose other than for which it was collected unless the individual has consented to such use, **unless**:

- The other purpose is directly related to the purpose for which the information was collected
- The use is necessary to prevent or lessen a serious and imminent threat to the life or health of the individual to whom the information relates, or to another person
- The use is reasonably necessary for another lawful and proper function of council (The Privacy Code of Practice for Local Government provides this exemption)
- Where personal information is to be used for the purpose of conferring an award, prize, benefit or similar form of personal recognition (The Privacy Code of Practice for Local Government provides this exemption)
- Compliance is reasonably likely to detrimentally affect, or prevent the proper exercise of conduct of a lawful Council investigation.

Some information collected by Council may be used for a variety of purposes.

For example, the names and addresses of individual owners of property kept as part of Council's rates records may be used to notify adjoining owners of proposed developments, to identify companion animal ownership, evaluate road openings and obstructions, evaluate tree preservation orders, investigate parking controls, evaluate land dedications and laneway status and to notify residents and ratepayers of Council services and activities. Council maintains a database of email addresses for the delivery of rates notices, employee payroll advice and for other special purposes. These databases may be used for a variety of other purposes such as newsletters or other notifications.

Council will only use health information for the purpose for which it was collected; a directly related purpose that the person would expect; with the consent of the individual; to lessen or prevent a threat to public health or safety; for law enforcement purposes where an offence may have been committed; where required by another act or law; or in accordance with the Guidelines issued by the Minister for Health regarding the use of information for research or training purposes.

Council will seek to contractually bind people or organisations to comply with this principle:

- Consultants and contractors of Council
- The Council-owned businesses

- Members (including community members) of Advisory Committees and Sub-Committees, Park Committees, Neighbourhood Committees
- Penrith City Council Delegates.

Where any of these seek to use personal information of a person collected for one purpose for another purpose, they must obtain written consent from the person.

Council does not need to comply, where the use of the information for another purpose is reasonably necessary for law enforcement purposes or for the protection of the public revenue. (s23(4) of the PPIPA)

Further Council need not comply with the use of information for the purposes of:

(i) investigating or otherwise handling a complaint or other matter that could be referred or made to, or has been referred from or made by, an investigative agency

(ii) the use of the information concerned for a purpose other than the purpose for which it was collected is reasonably necessary in order to enable the Council to exercise its complaint handling functions or any of its investigative functions. (s24(2) of PPIPA)

(iii) where 'non-compliance is 'necessarily implied' or 'reasonably contemplated' under any Act or law. (s25(a) & (b))

(iv) in order to disclose to the Minister or Premier, any matter under their administration (s28(3)).

3.11 Limits on Disclosure of Personal Information - Information Protection Principle 11

Council will not disclose personal information to a person (other than the individual to whom the information relates) or other body, **unless:**

- The disclosure is directly related to the purpose for which the information was collected, and Council has no reason to believe that the individual concerned would object to the disclosure
- The individual concerned is reasonably likely to have been aware, or has been made aware in accordance with the Act, that information of that kind is usually disclosed to that other person or body
- Council believes on reasonable grounds that the disclosure is necessary to prevent or lessen a serious and imminent threat to the life or health of the individual concerned or another person
- The individual expressly consents to the disclosure, for example, Council may provide information about an employee or former employee to a potential employer, or verify details concerning salary or wages to a financial institution where the person concerned has consented (s26(2))
- Required or permitted by another Act or law
- Documents are subpoenaed for production in a Court; personal information may be contained in those documents (s23(5)©)
- It is provided to Federal and NSW Police Services where required or permitted to do so or where there are reasonable grounds to believe an offence has been committed or to ascertain the whereabouts of a missing person (s23(5) of the PPIPA)
- It is provided to another NSW public sector agency or public utility where the agency has approached Council in writing, Council is satisfied that the information is to be used for a proper and lawful function/s and that the information is reasonably

necessary for the exercise of that agency's function, for example, electricity and water utilities and the NSW Electoral Commission seek details from Council of property owners in particular localities
- Information is to be disclosed for the purpose of conferring upon that person an award, prize, benefit or similar form of personal recognition
- Disclosure is for the protection of public revenue
- For the purposes of investigation of a complaint, or has been referred from another investigative agency (s24(4)).

Suppression

Information held by Council may be suppressed such as to disallow disclosure that would otherwise be allowed in the circumstances outlined above. See Part 1 of this Plan for more details about suppression of personal information.

3.12 Special Restrictions on Disclosure of Personal Information – Information Protection Principle 12

Council will not disclose personal information relating to an individual's ethnic or racial origin, political opinions, religious or philosophical beliefs, trade union membership, health or sexual activities unless the disclosure is necessary to prevent a serious or imminent threat to the life or health of the individual concerned or another person.

For the purposes of section 19(2), where Council is requested by a potential employer outside New South Wales, it may verify that:

(i) a current or former employee works or has worked for Council
(ii) the duration of their employment
(iii) the position occupied during their employment. This exception shall not permit Council to give an opinion as to that person's suitability for a particular position with any potential employer unless Council is satisfied that the person has provided their consent for Council to provide a reference, which may include an opinion as to that person's suitability for the position for which he/she has applied.

3.13 Additional Health Information Privacy Principles

Council will only collect health information for a lawful purpose that is directly related to Council's activities and is necessary for that purpose (HPP 1)

Council will ensure that the health information is relevant, accurate, up to date and not excessive and that the collection is not unnecessarily intrusive into the personal affairs of the individual (HPP 2).

Council will only collect health information directly from the individual that the information concerns, unless it is unreasonable or impractical for Council to do so. (HPP 3).

Council will tell the person why the health information is being collected, what will be done with it, who else might see it and what the consequences are if the person decides not to provide it. Council will also tell the person how he or she can see and correct the health information. (HPP 4)

If Council collects health information about a person from someone else, Council will take reasonable steps to ensure that the subject of the information is aware of the above points (HPP 5).

These are special requirements regarding giving of notice when health information is collected from a third party. Council will comply with the Statutory Guidelines approved by the Minister for Health regarding the giving of notice in these circumstances.

There are additional Health Privacy Principles contained in HRIPA concerning:

Principle 12:	The use of identifiers in the handling of health information
Principle 13:	The provision of a health service on the basis of anonymity
Principle 14:	Transfers of health information outside New South Wales or to a Commonwealth Government agency
Principle 15:	The inclusion of health information in a state or nationwide linked system

Council does not use identifiers in the handling of health information, does not currently provide a health service, or participate in any linked health record system.

Council will only transfer health information outside NSW or to a Commonwealth Government body where satisfied that this is required by law, or otherwise is in accordance with the provisions of HRIPA.

Council will provide details about what health information Council is holding about an individual and with information about why Council is storing that information and what rights of access the individual has (HPP 6).

Council will allow the individual to access his or her health information without reasonable delay or expense (HPP 7).

Council will allow the individual to update, correct or amend his or her health information where necessary (HPP 8).

Council will make sure that the health information is relevant and accurate before using it (HPP 9).

Council will only use the health information for the purpose for which it was collected or for a directly related purpose that the individual to whom the information relates would expect. Otherwise, Council will obtain the individual's consent (HPP 10).

Council will only disclose health information under the following circumstances:

- With the consent of the individual to whom the information relates; or
- For the purpose for which the health information was collected or a directly related purpose that the individual to whom it relates would expect; or
- If an exemption applies (HPP 11).

Council will only give an identification number to health information if it is reasonably necessary for Council to carry out its functions effectively (HPP 12).

PART 4 – COMPLIANCE

4.1 Compliance Strategy

During induction and when changes occur, all employees will be made aware of this Plan and it will be made available on Council's intranet and website.

Councillors, employees, contractors and volunteers will be either given or provided access to the PMP.

4.2 Responsibilities of the Privacy Contact Officer

Council's Public Officer is the person responsible for managing privacy related issues. This involves provision of information and advice about legislative obligations and the privacy implications of new projects, plans, initiatives or policies; dealing with enquiries from the public; managing or undertaking investigations of complaints; and reviewing Council policy, procedures and this Plan.

Internet contact forms, rates notices, application forms, or written requests by which personal information is collected by Council must be referred to the Public Officer before they are adopted or used.

The Public Officer will also provide the following advice:

- whether the personal information is collected for a lawful purpose
- if the purpose relates to a direct function of Council
- whether or not the collection is reasonably necessary for a specified purpose.

The Public Officer will ensure that Council has special provisions in its public areas for working with computer screens. These may include:

- fast screen savers
- facing the screens away from the public
- only allowing the records system to show one record at a time.

Council will ensure that electronic databases are reviewed to ensure that they contain procedures and protocols to check the accuracy and currency of personal and health information.

Council's annual report will include details of GIPA Act requests.

A copy of the current edition of Council's PMP is published on Council's website.

Should the Council require, the Privacy Contact Officer may assign designated officers as 'Privacy Resource Officers', within the larger departments of Council. In this manner the Council may ensure that the information protection principles are more broadly understood and that individual departments have a greater focus on the information protection principles and are directly applied to Council's day to day functions.

PART 5 – INTERNAL REVIEW

5.1 Dissatisfaction with the way Council has dealt with Privacy

Council's Privacy Contact Officer can assist with enquiries about privacy issues and can be contacted through Council Offices.

Any person is entitled to any personal information that Council holds about them. They may request alterations be made to their personal details or request information on the way their personal details have been used.

If an individual is not satisfied with Council's conduct in relation to their privacy request, disclosure of personal information on a public register or believe Council is contravening a privacy principle or privacy code of practice they can make an application for internal review of Council's conduct or decision by writing to Council's Privacy Contact Officer.

Council's Privacy Contact Officer
Penrith City Council
PO Box 60, PENRITH NSW 2751
Telephone: 02 4732 7777
Email: council@penrith.city

The written application must be addressed to Council, include a return postal address or email address and be received by Council within 6 months of the individual becoming aware of the conduct or decision that is the subject of the application.

Any complaint should provide sufficient detail of the alleged infringement to enable Council to investigate. The complaint will then be forwarded to the Privacy Contact Officer for review. Council will undertake an investigation and inform the NSW Privacy Commissioner that a complaint has been received.

5.2 How does the process of Internal Review operate?

The Privacy Contact Officer will appoint a Reviewing Officer to conduct the internal review. The Reviewing Officer will report their findings to the Privacy Contact Officer. The review is to be completed within 60 days of receipt of the application. The applicant will be notified of the outcome of the review within 14 days of its determination.

The Privacy Commissioner will be notified by the Privacy Contact Officer of a review application as soon as is practicable after it is received. Council will brief the Privacy Commissioner on the progress of an internal review and notify them of the outcome.

5.3 The Role of the Privacy Commissioner in the Internal Review process

The Privacy Commissioner may make submissions to Council in relation to the subject matter of the application for internal review. Council may, if it deems it appropriate, ask the Privacy Commissioner to conduct the internal review (s53, PPIPA).

5.4 What happens after an Internal Review?

If the applicant remains dissatisfied with the outcome of a review or the review has not been completed within 60 days, an application may be made to the Civil Administration Tribunal for a review of Council's conduct (s55).

If the applicant is dissatisfied with an order or decision made by the Tribunal, they may make an appeal to an Appeal Panel of the Tribunal.

PART 6 – DATA BREACH POLICY

6.1 What we will do if there has been a Data Breach

If a serious data breach has been identified, we will notify the affected individuals, parties and Privacy Commissioner. A serious data breach is defined as unauthorised access to, unauthorised disclosure of, or loss of, personal information and/or health information held by

us, and as a result of this breach, there is a real risk of serious harm to any of the individuals to whom the information relates.

Data breaches may result in unauthorised collection, use, disclosure or access to personal information. If a serious data breach occurs, Penrith City Council will act quickly to contain the breach, evaluate the risks, notify the affected individuals and work to prevent this happening again.

Council believes it is important that individuals are aware that their personal information has been breached, so the affected persons can take steps to mitigate any loss or damage as a result of a breach.

We will also notify the Information Privacy Commissioner of such a breach.

6.2 What should you do if you suspect a Data Breach

If you suspect that there has been a breach of personal information, you should contact Council's Right to Information Officer immediately. When contacting Council's Right to Information Officer please provide a brief description of the breach, including when the breach occurred, how it occurred, what data was affected, how long the data was affected and what type of breach, e.g loss, disclosure or unauthorised access. Please provide the above information in writing via email to council@penrith.city for action.

6.3 NSW public sector agencies and notifiable data breaches (NDB)

The Notifiable Data Breaches (NDB) scheme, under the federal Privacy Act 1988 (Privacy Act), came into effect on 22 February 2018. Fact sheet - NSW Public Sector Agencies and Notifiable Data Breaches February 2018

The NDB scheme establishes a mandatory data breach notification scheme that requires organisations covered by the federal Privacy Act to notify individuals likely to be at risk of serious harm due to a data breach.

Although the NDB scheme is aimed primarily at federal government agencies and private sector organisations regulated by the Australian Privacy Principles (APPs) under the Privacy Act, there are provisions that apply to NSW public sector agencies.

As an agency that collects tax file numbers (TFNs), Council has an obligation under the NDB scheme when a data breach occurs involving a TFN.

The Privacy (Tax File Number) Rule 2015 (TFN Rule)1 issued under s.17 of the Privacy Act, regulates the collection, storage, use, disclosure, security and disposal of individuals' TFN information. The TFN Rule requires any organisation holding TFNs to protect the information by implementing reasonable security safeguards in the circumstances.

The obligations under the TFN Rule are in addition to responsibilities under other laws, such as the PPIPA.

Council will comply with its legal obligations where a data breach involves a TFN. Those obligations are appended to this PMP.

6.4 NSW public sector agencies and mandatory notifiable data breaches (MNDB)

The Mandatory Notification of Data Breach Scheme (MNDB scheme) came into effect on 28 November 2023 - Mandatory Notification of Data Breach Scheme: Exemptions from notification requirements

The MNDB requires public sector agencies bound by the Privacy and Personal Information Protection Act 1998 (PPIP Act) to notify the Privacy Commissioner and affected individuals of data breaches of personal or health information likely to result in serious harm.

The MNDB scheme will require public sector agencies to notify the Privacy Commissioner and affected individuals if a data breach affecting personal or health information that is likely to result in serious harm occurs. Council are also required to maintain an internal data breach incident register and have a publicly accessible data breach policy.

6.5 Why is the proposed MNDB scheme so similar to the NDB scheme?

The development of the MNDB scheme was informed by the experiences of the NDB scheme. New South Wales frequently shares information with the Commonwealth and would benefit from similar data breach notification schemes. In some limited instances, breaches may be captured by both schemes. Breaches of tax file numbers are reportable under the NDB scheme. They may also be notifiable under the MNDB scheme if the breach occurred within a NSW public sector agency and was likely to result in serious harm.

Importantly, data breaches affect agencies broadly; a breach that compromises tax file numbers will often compromise other personal and health information. The MNDB scheme has been designed to adopt, as far as possible, key features of the NDB scheme to limit the impact of this overlap.

6.6 Councils Right to Information Officers (RIO) Responsibilities:

The MNDB scheme requires public sector agencies to notify the Privacy Commissioner and affected individuals if a data breach affecting personal or health information that is likely to result in serious harm occurs.

Council's RIO will conduct a review and determine if the subject information is likely to result in serious harm. If the information is likely to do so, Councils RIO will notify the Privacy Commissioner and affected individuals.

Council's RIO is also required via the MNDB scheme to satisfy other data management requirements, including to maintain an internal data breach incident register, and to regularly update Councils data breach policy within this PMP.

PART 7 – OTHER RELEVANT MATTERS

7.1 Regular review of Privacy Management Plan

When information practices are reviewed from time to time, the Privacy Management Plan will also be reviewed to ensure that the Plan is up to date.

7.2 Further Information

For assistance in understanding the processes under the PPIPA and HRIPA, please contact the Council.

Penrith City Council PO Box 60, PENRITH NSW 2751 Telephone: 02 4732 7777 Email: council@penrith.city	Information and Privacy Commission GPO Box 7011, SYDNEY, NSW 2001 Telephone: 1800 472 679 Email: ipcinfo@ipc.gov.au

7.3 Investigative Functions

Where Council is conducting an investigation, it will have regard to any applicable Direction of the Privacy Commissioner under s 41 of the PPIPA that may affect the application of Information Protection Principles.

Any use of information for the purposes of research will be in accordance with the Direction issued by the NSW Privacy Commissioner.

APPENDIX: NSW Public Sector Agencies and Notifiable Data Breaches – Fact sheet

information and privacy commission new south wales

NSW Public Sector Agencies and Notifiable Data Breaches

Fact sheet
February 2018

The Notifiable Data Breaches (NDB) scheme, under the federal *Privacy Act 1988* (Privacy Act), comes into effect on 22 February 2018.

The NDB scheme establishes a mandatory data breach notification scheme that requires organisations covered by the federal Privacy Act to notify individuals likely to be at risk of serious harm due to a data breach.

Although the NDB scheme is aimed primarily at federal government agencies and private sector organisations regulated by the Australian Privacy Principles (APPs) under the Privacy Act, there are provisions that apply to NSW public sector agencies.

Tax file number collection

Any agency that collects tax file numbers (TFNs) has obligations under the NDB scheme when a data breach occurs involving a TFN. This includes state and local government agencies, and public universities in NSW that routinely collect and hold TFN information.

A TFN is a unique number issued by the Australian Taxation Office (ATO) to identify individuals. TFN information is information that connects a TFN with the identity of a particular individual.

The *Privacy (Tax File Number) Rule 2015* (TFN Rule)[1] issued under s.17 of the Privacy Act, regulates the collection, storage, use, disclosure, security and disposal of individuals' TFN information. The TFN Rule requires any organisation holding TFNs to protect the information by implementing reasonable security safeguards in the circumstances.

The obligations under the TFN Rule are in addition to responsibilities under other laws, such as the *Privacy and Personal Information Protection Act 1998* (PPIP Act).

What is a TFN data breach?

A TFN data breach occurs where TFN information is lost, or subject to an unauthorised access or disclosure.

There are a number of ways this can occur. For example, if a database containing TFN information is hacked, if a TFN is mistakenly provided to the wrong person, or when paper records containing any TFN information are stolen.

When is a TFN data breach 'notifiable'?

The notification requirements under the NDB scheme will be triggered if the TFN data breach is 'likely to result in serious harm' to any individual.

Responding to a TFN data breach

Each TFN data breach will have to be dealt with on a case-by-case basis. However, there are four key steps to consider when responding to a breach:

1. Contain the breach

Depending on the type of TFN data breach, containing the breach may involve a range of responses. This could include searching for and recovering the TFN data, confirming that no copies were made or that the information was destroyed by the party receiving it, conducting a remote wipe on a lost portable device, implementing a computer system shut down, or changing passwords and system user names.

When a TFN data breach occurs you should conduct preliminary fact-finding about the breach (including cause, risk of spread, options to mitigate risk) and assess the risk posed by the breach.

It is important to inform the relevant key people in your organisation of the breach, such as the Privacy Officer and the Chief Executive Officer. In certain circumstances, it may also be necessary to inform the police.

2. Evaluate and mitigate the risks

Taking prompt remedial action will minimise the likelihood that the breach will result in harm to any individual. For example, depending on the type of data breach, employees might be told to change passwords, not to open emails with attachments, and to be aware of phishing attacks.

An assessment of the likely harm resulting from a TFN breach should be conducted as soon as practicable after an agency becomes aware of the breach. Ideally this will occur within 2-3 days but all reasonable steps must be taken to ensure the assessment is completed within 30 days.

The assessment should determine whether your agency reasonably believes that the loss, access or disclosure is 'likely to result in serious harm to any of the individuals to whom the information relates'. 'Serious harm' is not defined in the Privacy Act, but guidance from the Australian Privacy Commissioner suggests that it could

[1] https://www.legislation.gov.au/Details/F2015L00249

include such things as serious financial, physical, psychological, emotional or reputational harm.

3. Notification and communication

When the assessment at step 2 has been completed, notification (if required) must be commenced as soon as practicable.

Notification is required by law if the assessment has concluded that there are reasonable grounds to believe that the breach has resulted in, or is likely to result in, serious harm to one or more of the individuals to whom the information relates.

The notification requirements relate to notifying both the Australian Privacy Commissioner and the affected individuals.

A statement must be prepared about the TFN data breach which sets out the following:

- Identity and contact details of the agency that experienced the breach
- A description of the breach
- The kind or kinds of information concerned
- Recommendations about any steps that the individuals should take in response to the breach.

The statement may also include:

- any action that has been, or is being taken, to rectify the breach and mitigate any harm;
- details about any other party that has been notified (e.g. the NSW IPC or NSW Police); and
- if relevant, the identity and contact details of any other related organisations that are likewise affected by the data breach.

The statement must be sent to the Australian Privacy Commissioner at the Office of the Australian Information Commissioner (OAIC) as soon as practicable.

The statement must also be provided to the affected individuals as soon as practicable. As a minimum requirement, the statement must be:

1. provided directly to only those individuals at risk of serious harm; or
2. provided to all individuals whose TFN information was breached; or
3. (only if the affected individuals cannot be contacted directly) publicised more broadly.

This notification can be in the form of an email, letter or by phone contact. Additional steps may include a dedicated website, a media release or posts on social media.

Note: If NSW Police or another law enforcement agency is investigating the breach, they must be consulted before making details of the breach public.

4. Prevention of future breaches

Following a TFN data breach, agencies should fully investigate the cause of the breach and consider developing a prevention plan.

To mitigate the risk of any future data breaches, agencies may take a range of steps, including:

- a security audit and any modifications to physical controls such as locks, alarms, visitor access control;
- a review of policies and procedures including the privacy management framework;
- a review of employee training;
- a review of suppliers and third parties; and
- updating passwords, or altering deployments of technology.

More information about TFN data breaches

The OAIC has a dedicated website for the NDB scheme – see https://www.oaic.gov.au/privacy-law/privacy-act/notifiable-data-breaches-scheme.

In addition, further information about the handling of TFN information is available at: https://www.oaic.gov.au/privacy-law/privacy-act/tax-file-numbers.

To contact the OAIC, call 1300 363 992 or email enquiries@oaic.gov.au.

Other data breach notification schemes

In addition to the NDB scheme, there are two other data breach notification schemes which create responsibilities for NSW public sector agencies in certain circumstances.

A. Sharing of government sector data

The *Data Sharing (Government Sector) Act 2015* (DSGS Act) has a data breach notification scheme in respect of sharing of government sector data under the DSGS Act with the NSW Data Analytics Centre, or between other government sector agencies.

If an agency that is receiving personal or health information under the DSGS Act becomes aware that privacy legislation has been (or is likely to have been) breached, the agency must, as soon as practicable, inform the data provider and the NSW Privacy Commissioner (IPC) of the breach.

B. European Union's General Data Protection Regulation

The *General Data Protection Regulation* (GDPR) will apply from 25 May 2018 to any organisation offering goods or services to, or monitoring the behaviour of, individuals living in the European Union (EU). This may include some NSW public sector agencies (e.g. universities offering educational packages to international students).

The data breach notification requirements under the GDPR include notification to the relevant EU supervisory authority within 72 hours after having become aware of the breach.

Further information is available from the OAIC.

Notification of data breaches to the IPC

As a matter of best practice, agencies are encouraged to voluntarily report all other types of data breaches to the IPC, and to affected individuals as appropriate. This may include data breaches involving personal information other than TFNs, or data breaches involving TFNs but which are *not* likely to result in serious harm.

Notification should contain similar content to that provided to individuals/organisations. The personal information about the affected individuals is not required. It may be appropriate to include:

- a description of the breach;
- the type of personal information involved in the breach;
- what response the agency has made to the breach;
- what assistance has been offered to affected individuals;
- the name and contact details of the appropriate contact person; and
- whether the breach has been notified to other external contact(s).

Having a data breach procedure or policy can make it easier to handle a data breach. The IPC has proactively released its *IPC Data Breach Policy* and agencies are encouraged to refer to it when reviewing their own policies. The *IPC Data Breach Policy* is available on the IPC website.

For more information

Contact the Information and Privacy Commission NSW (IPC):

Freecall: 1800 472 679
Email: ipcinfo@ipc.nsw.gov.au
Website: www.ipc.nsw.gov.au

information and privacy commission new south wales
www.ipc.nsw.gov.au | 1800 IPC NSW (1800 472 679)

Appendix: Fact Sheet - Mandatory Notification of Data Breach Scheme: Exemptions from notification requirements

information and privacy commission new south wales

Fact Sheet **March 2023**

Mandatory Notification of Data Breach Scheme: Exemptions from notification requirements

The Mandatory Notification of Data Breach Scheme ('MNDB Scheme') was created by amendments to the *Privacy and Personal Information Protection Act 1998* (NSW) (PPIP Act) and will commence on 28 November 2023.

The MNDB Scheme requires that NSW public sector agencies ('agencies') notify affected individuals and the Privacy Commissioner when there has been an 'eligible data breach'.

You can find more information about the MNDB Scheme here.

When does an agency need to notify individuals about an eligible data breach?

When a data breach occurs, an agency must immediately make all reasonable efforts to contain the breach and try to reduce the likelihood that an individual will experience serious harm.

Agencies then have 30 days from the date they become aware of a possible data breach to assess whether that data breach is an eligible data breach. This assessment should be carried out as expeditiously as possible. Whilst making this assessment, all reasonable attempts must be made to mitigate any harm already done.

Once an agency decides there has been an eligible data breach, the agency must notify the affected individuals as soon as practicable about that breach, with limited exceptions.

When would an agency not be required to notify an affected individual?

Part 6A, Division 4 of the PPIP Act provides a limited number of exemptions from the requirement to notify affected individuals of an eligible data breach. An agency will not be required to notify where any of the following exemptions apply.

Breaches involving multiple agencies

The exemption under section 59S will apply where:

- the data breach involves more than one agency,
- each agency has undertaken an assessment of the breach,
- the head of each agency has made a data breach notification to the Privacy Commissioner, and
- the other agency involved in the breach has undertaken to notify affected individuals of the eligible data breach.

Agencies should work together during the assessment process to ensure all affected individuals are identified.

The notification provided to the affected individuals should identify all agencies involved in the breach. The notification should also identify a central contact for further enquiries.

This exemption would not apply where multiple entities were involved in the breach but only one entity was an agency. In this instance, the agency would need to comply with the notification requirements even if another entity (including an agency of the Commonwealth or another state or territory) was also required to notify affected individuals under Commonwealth or other law.

Investigations and legal proceedings

The exemption under section 59T will apply where the agency reasonably believes notification would likely prejudice:

- an investigation that could lead to the prosecution of an offence
- proceedings before a court or tribunal
- another matter prescribed by regulations.

Mitigation of harm

The exemption under section 59U will apply where the agency:

- takes action to mitigate the harm done by the breach, and

- the action is taken before the breach results in serious harm to an individual, and
- because of the action taken, a reasonable person would conclude that the breach would not be likely to result in serious harm to the individual.

The time period for when this exemption could apply is *after* the agency has determined that the breach is an eligible data breach but *before* the breach results in serious harm to the individual.

Secrecy provisions

The exemption under section 59V will apply where compliance by the agency with the notification requirements would be inconsistent with a secrecy provision.

For the purposes of the MNDB Scheme, a secrecy provision means a provision of an Act or statutory rule that prohibits or regulates the use or disclosure of information.

Serious risk of harm to health or safety

The exemption under section 59W will apply where the agency reasonably believes that notification would create a serious risk of harm to an individual's health or safety.

When considering whether to apply this exemption the agency must have regard to the Privacy Commissioner's Guideline on the exemption under section 59W.

When making a decision to apply this exemption the agency must:

- consider the extent to which the harm that may be caused by notifying the individual is greater than the harm of not notifying the individual about the breach, and
- consider the currency of the information relied on in assessing the serious risk of harm to the individual, and
- must not search data held by the agency that was not affected by the data breach during the assessment of risk unless the agency knows, or reasonably believes, there is information in the data that is relevant to whether the exemption applies.

This exemption can be applied permanently, temporarily or until a particular event has occurred. The type of exemption applied will depend on the nature and context of the breach and the unique characteristics and circumstances of the affected individual.

The agency must provide a written notice to the Privacy Commissioner where this exemption is relied upon. The notice must include the information specified under section 59W(5).

Cyber security

The exemption under section 59X will apply where the agency reasonably believes that notification would:

- worsen the agency's cyber security, or
- lead to further data breaches.

When considering whether to apply this exemption the agency must have regard the Privacy Commissioner's Guideline on the exemption under section 59X.

This exemption can only be applied on a temporary basis for the duration of the risk to the agency's cyber security.

The agency must provide a written notice to the Privacy Commissioner where this exemption is relied upon. The notice must include the information specified under section 59X(3).

The agency must review the use of this exemption each month and provide an update to the Privacy Commissioner.

Notification to the Privacy Commissioner

The exemptions set out in Division 4 of the PPIP Act **do not** affect an agency's obligation to make a notification to the Privacy Commissioner under section 59M.

For more information

Contact the Information and Privacy Commission NSW (IPC):

Freecall: 1800 472 679
Email: ipcinfo@ipc.nsw.gov.au
Website: www.ipc.nsw.gov.au