NOOSA Council	Council Policy **PRIVACY POLICY**
Corporate Plan Reference:	Theme 5: Excellence 5.5 Provide robust and transparent governance systems to build and strengthen community trust, supported by the implementation of an enterprise risk and opportunity management framework.
Endorsed by Council:	19 December 2024
Policy Author:	Governance Manager

POLICY STATEMENT

Noosa Shire Council (Council, 'we', 'us', 'our') collects and handles significant amounts of personal information. Council is committed to protecting an individual's personal information and right to privacy. Council is committed to the collection, use, disclosure, storage, and management of personal information in accordance with the Queensland Privacy Principles (QPPs) contained in Schedule 3 of the Queensland *Information Privacy Act 2009* (IP Act) and other privacy provisions in the IP Act.

PURPOSE

The purpose of this Policy is to explain how Council collects and manages the personal information of individuals. In other words, Council adheres to the IP Act by providing for the fair collection and handling of personal information.

SCOPE

This Policy applies to Councillors, all Council employees, volunteers and authorised non-Council employees (e.g., contractors) who conduct activities and functions on behalf of Council and are involved in the collection, use, disclosure, and storage of personal information (collectively referred to as '**employees'**).

REVIEW

This Policy will be reviewed once per Council term (every four years) or as required from time to time.

COUNCIL POLICY

What is privacy?

Privacy relates to the protection of personal information in accordance with the IP Act and community expectations.[1]

[1] OIC, *Privacy in Local Government: An Introduction to meeting obligations under the Information Privacy Act 2009*, 2022, p. 2.

More broadly, privacy is also a protected human right under the Queensland *Human Rights Act 2019*[2] and this right protects the privacy of people in Queensland from unlawful or arbitrary interference.

What is personal information?

Personal information is defined as:

> '*Information or an opinion about an identified individual or an individual who is reasonably identifiable from the information or opinion –*
> *(a) whether the information or opinion is true or not, and*
> *(b) whether the information or opinion is recorded in a material form or not.*'[3]

In general terms, personal information is any information that can be used to identify an individual.

An individual does not need to be directly identified for the information to be 'personal information'. It is sufficient if they can reasonably be identified by reference to other information.[4]

What is not personal information?

The QPPs do not apply to information that is publicly available, for example, information in annual reports, corporate plans, or the Queensland Government Gazette.

Why does Council collect personal information?

Council collects personal information of individuals for a range of reasons, including, but not limited to:

a) provide services
b) notify a person about services
c) issue rates notices
d) undertake public consultation on a range of Council matters
e) provide customer service functions, including handling customer enquiries and complaints and,
f) process enquiries an individual has submitted to Council, including contacting, and providing a person with information in relation to their enquiry.

How does Council collect personal information?

Council will only collect personal information when it is necessary for the particular function or activity that is being carried out by Council. Therefore, personal information may be collected by Council in the following ways:

a) directly from an individual, for example, when Council requests personal information from a person through forms or at a customer service counter, or
b) through an individual's authorised representative, for example, a lawyer, or
c) through third parties, including, other government agencies, or
d) through available databases, for example, Council's Land Register, or
e) through Council's websites (refer to Website Privacy Policy for further information), or
f) through email lists, subscriptions, newsletters, or events an individual signs up to with Council, or

[2] *Human Rights Act 2019* (Qld), s 25.
[3] *Information Privacy and Other Legislation Amendment Act 2023* (Qld), s 12.
[4] Office of the Information Commissioner Queensland, *IPOLA Guideline: QPP 3&6 – Permitted General Situations*, version 1.0, June 2024, p. 1.

g) through social media services, such as Facebook or LinkedIn.

Collection Notices

All forms used by Council to collect personal information, such as the Online Rates Form, will generally carry the following notice:

> *Council will use any personal information provided for the intended purpose only, to remain in contact with you regarding the legitimate functions and services affecting your property and to continually improve your customer service experience. Council is authorised to collect this information in accordance with the Local Government Act 2009 and other local government Acts. These details will not be provided to third parties and are only accessed by persons authorised to do so. Your personal information is handled in accordance with Council's Privacy Policy.*

The collection notice may be modified to include additional or changed information where it is necessary and appropriate to do so in order to make an individual generally aware of:

a) why the information is being collected
b) details of any law that specifically allows or requires the collection, and
c) any entity to who it is the Council's usual practice to give the information to, and (if known) anyone who they will in turn give it to.

What types of personal information are collected and held by Council?

The types of information Council may collect and hold about a person will depend on how a person interacts with Council or the services Council are providing to a person.

Some examples of the types of personal information Council typically collects and holds includes:

- full name and contact details, including a person's email address and phone number (landline and mobile)
- date of birth
- postal address
- land address
- gender
- driver licence, passport or other documents that evidence a person's identity
- occupation, employment history and educational background
- personal information provided by individuals using Council's complaint management system, including details of the complainant, subject of the complaint, witnesses etc., and
- personal information provided during recruitment processes (e.g., curriculum vitae or referees).

How does Council use an individual's personal information?

Under the IP Act, Council may only use an individual's personal information for the purpose for which it was collected. However, Council may use an individual's personal information for another purpose where:

a) a person has expressly or impliedly agreed to their personal information being used for the other purpose, or
b) the other purpose is directly related to the original purpose we collected the information, or
c) use of the information for the other purpose is necessary to protect the life, health, safety or welfare of an individual or the public, or
d) use of the information for the other purpose is authorised by law, or

e) use of the information for the other purpose is required for law enforcement purposes, or
f) use of the information is necessary for research or statistical purposes, with some limitations.

Does Council disclose an individual's personal information?

In order for Council to provide a person with services and undertake functions and responsibilities, Council may be required to disclose an individual's personal information to third parties. However, Council will only disclose an individual's personal information if:

a) a person has expressly or impliedly consented to the release, or
b) Council has made a person aware that it is Council's usual practice to disclose the information to a third party, or
c) the disclosure is necessary to lessen or prevent serious threat to life, health, safety, or welfare of the public or an individual, or
d) the disclosure is authorised or required under a law, or
e) the disclosure is necessary for law enforcement purposes, or
f) the disclosure is necessary for research or statistical purposes, with some limitations.

Some examples of when Council may disclose an individual's personal information include:

- if a person has lodged a complaint with a complaint body and they are conducting a review, for example, the Queensland Ombudsman, or
- if a law enforcement agency requires the information for the purposes of an investigation, or
- in a disaster or emergency event, Council may pass on the personal information of individuals to other emergency service agencies for emergency response purposes, or
- under the Queensland *Planning Act 2016* which requires that Council publish online, the names of development proponents and submitters at certain points of the development application process.

Council will take all reasonable steps to ensure the third-party recipient of an individual's personal information will not use or disclose the information for a purpose other than the purpose for which it was disclosed by Council.

How does Council store an individual's personal information?

Council will take all reasonable steps to ensure personal information is protected from loss, unauthorised access, use, modification or disclosure and any other misuse. Council may hold personal information in either secure electronic record keeping systems or hard copy form. Where reasonable and practicable to do so, personal information is destroyed or de-identified when no longer needed and in accordance with the Queensland *Public Records Act 2002*.

How do contracted service providers deal with personal information?

Occasionally, Council may enter into contracts with service providers for the performance of our functions. If an individual's personal information is required, for any reason, to be disclosed to those service providers, Council will take all reasonable steps to ensure that the service provider is bound by the same rules and regulations that bind Council in relation to the collection, use, disclosure, and storage of personal information under the IP Act. Once bound, the service provider is responsible for any breach of the privacy rules under the IP Act and individuals can make privacy complaints directly against the provider.

Can personal information be transferred outside Australia?

Council will only transfer an individual's personal information outside Australia if it is required for a legitimate purpose and only if:

a) a person consents to the transfer, or
b) the transfer is authorised or required under a law, or
c) the transfer is necessary to lessen or prevent serious threat to the life, health, safety, or welfare of the public or an individual, or
d) two or more of the following apply –
    i. the recipient is subject to equivalent privacy obligations, or
    ii. the transfer is necessary to perform a function of Council, or
    iii. the transfer is for a person's benefit, or
    iv. reasonable steps have been taken by Council to ensure the information will not be held, used, or disclosed in a manner that is inconsistent with the IP Act.

Does Council use surveillance technologies that capture personal information?

Council may use surveillance technologies, such as closed-circuit television (CCTV), body worn cameras, drones, and sensors/cameras on council vehicles, to attend to several Council functions, including safeguarding assets, local laws enforcement, Shire management and planning, environmental assessments, land use surveys and community engagement. As such, Council is required to comply with the IP Act when our surveillance technology collects personal information.

When using surveillance technologies, Council will ensure that:

a) the collection of personal information by surveillance technologies is necessary for the purpose of the project and/or work[5]
b) where practicable, people are provided with a Collection Notice before their image or other personal information is collected using surveillance technologies (or as soon as practicable after the collection)[6]
c) surveillance footage, voice recordings and other data are protected against loss, unauthorised access, use, modification or disclosure, or any other misuse[7]
d) anyone can apply to access information included in footage, voice recordings and other data collected by surveillance technologies,[8] and
e) surveillance footage, voice recordings and other data that contain personal information are only used and disclosed for the purpose that they were collected for.[9] Where footage is to be used or disclosed for another purpose, Council will determine whether an exception set out in QPP 6[10] applies.

How can a person access or amend their personal information held by Council?

A person has the right to request access to or amend their personal information held by Council. There are several ways this can be achieved as outlined below.

Administrative Access

In some cases, personal information of individuals can be released without the need for a formal application under the IP Act. Council's Administrative Access Scheme provides further information about when Council may release information administratively.

Please contact Council's Governance Branch via the contact details below for advice on whether personal information can be released administratively.

[5] Refer to *Information Privacy and Other Legislation Amendment Act 2023* (Qld), s 74, QPP 3.1.
[6] Refer to *Information Privacy and Other Legislation Amendment Act 2023* (Qld), s 74, QPP 5.
[7] Refer to *Information Privacy and Other Legislation Amendment Act 2023* (Qld), s 74, QPP 11.
[8] Refer to *Information Privacy and Other Legislation Amendment Act 2023* (Qld), s 74, QPP 12 and Chapter 3 of the IP Act.
[9] Refer to *Information Privacy and Other Legislation Amendment Act 2023* (Qld), s 74, QPPs 6.
[10] *Information Privacy and Other Legislation Amendment Act 2023* (Qld), s 74.

Application under the IP Act

The IP Act gives individuals the right to access their personal information held by government agencies. A person can make a formal application under the IP Act for access to their personal information by downloading and completing the IP Application Form available on Council's website. There is no fee associated with this application. Further details can be found here. Please send the completed form to Council's Governance Branch via the contact details below.

Amending personal information

Council takes all reasonable steps to ensure the personal information held about an individual is current and accurate. However, if a person believes that their personal information held by Council is:

a) inaccurate
b) misleading
c) out of date, or
d) incomplete

they can apply to have their personal information amended under the IP Act.

Individuals can apply to amend their personal information held by Council by downloading and completing the IP Amendment Form. There is no fee associated with this application. Further details on how to amend personal information can be found here.

Amendment applications should contain:

a) details of the information an individual wants to amend,
b) why an individual believes the information is inaccurate, misleading, out of date or incomplete,
c) the amendments the individual wants to be made, and
d) certified evidence of their identity.

Please send the completed form to Council's Governance Branch via the contact details below.

Privacy breaches

A privacy breach can occur when there is a failure to comply with one of the QPPs. Privacy breaches can occur for a range of reasons, such as human error, inadequate resources and training or technical problems. A privacy breach may include, but is not limited to:

- over-collection of personal information (i.e., collecting more than is necessary for a council function)
- failure to take reasonable steps to notify an individual about the collection of their information
- refusal to give an individual access to their own personal information where no exception can be applied
- unauthorised use of personal information internally by council, or externally by third parties
- unauthorised disclosure of personal information, including where personal information is provided to service providers that have not been adequately bound to relevant sections of the IP Act
- transfer of personal information outside Australia in a manner that does not comply with the IP Act
- improper application of QPP exceptions in relation to the collection, use and disclosure of personal information; or where council acts as though it is relying on an QPP exception where no exception applies.

Responding to breaches

Council will implement several key steps when responding and managing a privacy breach. We will:

1. **Contain** the breach – immediately take all reasonable steps to prevent any further compromise of personal information.
2. **Assess** the risk of serious harm by gathering information to assess the nature, extent, and severity of the breach, to best understand how to respond.
3. **Consider** whether mandatory notification of the affected individuals and the Information Commissioner is required (refer to Mandatory Notification of Data Breaches below).
4. **Notify** affected individuals (and the Queensland Office of the Information Commissioner) if required to do so.
5. **Review** the incident and the response to understand how to manage future breaches and strengthen systems and procedures.

It is Council practice to provide a Privacy Breach Report for all serious data breaches to the Queensland Office of the Information Commissioner (OIC) for transparency, legislative compliance and to alert the OIC that individuals affected by the breach may contact the OIC with complaints. Additionally, there is a specific process and timeframe required for serious data breaches pursuant to the IP Act that is set out below.

In response to a breach, Council may also implement its Data Breach Response Plan. This Plan has been prepared to comply with legislative requirements,[11] is set out in Appendix A and forms part of this Policy.

Mandatory Notification of Data Breaches

If the breach, or suspected breach, is an 'eligible data breach' under the IP Act, it must be assessed and reported to the OIC.

A breach will be an 'eligible data breach' where:

a) the data breach involves unauthorised access to, or unauthorised disclosure of personal information, and
b) the access or disclosure is *likely to cause serious harm* to an individual to whom the information relates.

The assessment of whether the data breach is likely to cause serious harm is done by reference to the following factors:

- the type of personal information accessed, disclosed, or lost, and
- the sensitivity of the personal information, and
- whether the personal information is protected by 1 or more security measures, and
- the likelihood that any security measures in place, could be overcome, and
- the persons, or the kinds of persons, who have obtained, or who could obtain the personal information, and
- the nature of the harm likely to result from the data breach.[12]

Therefore, 'serious harm' to an individual in the circumstances includes, for example, serious physical, psychological, emotional, or financial harm to the individual because of the access or disclosure, or serious harm to the individual's reputation because of the unauthorised access or disclosure.

[11] *Information Privacy and Other Legislation Amendment Act 2023* (Qld), s 73.
[12] Ibid., s 47.

In accordance with the IP Act, Council will have 30 days to assess if a breach or suspected breach is an 'eligible data breach'. During the assessment period, Council will continue to take all reasonable steps to contain the breach and mitigate the harm caused by the breach. Furthermore, any other agencies or organisations that may be affected by the data breach will be notified. If Council concludes that the event is an eligible data breach, a Privacy Breach Report will be provided to the OIC as soon as reasonably practicable after forming that conclusion and in accordance with legislative requirements.

Privacy Complaints

If a person believes that Council has not dealt with their personal information in accordance with the IP Act, they may make a privacy complaint. Privacy complaints must be made to Council within twelve months after the complainant becomes aware of the act or practice that is the subject of the complaint, or a longer period agreed to by Council.[13]

To lodge a privacy complaint with Council, please submit your complaint in writing via the Privacy Complaint Form. Upon receipt of the complaint, Council's Governance Branch will formally acknowledge the individual within five business days.

Complaints to the Office of the Information Commissioner

A person must lodge a privacy complaint with Council prior to applying to the OIC. However, a person can make a privacy complaint to the OIC if:

a) at least 45 business days have elapsed since the privacy complaint was made to Council, and
b) an extension of time beyond the initial 45 business days was not sought by Council, and
c) they have not received a response from Council, or they do not consider the response received is adequate.

Further information about OIC's privacy complaint process is available here.

Contact Us

To make an enquiry about how Council handles personal information, to access or amend your personal information or to make a privacy complaint, please contact the Governance Branch:

Webpage/s:	https://www.noosa.qld.gov.au/about-council/governance/right-to-information-and-privacy https://www.noosa.qld.gov.au/about-council/governance/complaints
Phone:	(07) 5329 6500
Email:	governance@noosa.qld.gov.au
Postal Address:	PO Box 141, Tewantin QLD 4565

ROLES AND RESPONSIBILITIES

Councillors

Councillors will consider and adopt Council's Privacy Policy.

When dealing with personal information, Councillors will comply with the IP Act and the associated QPPs contained in Schedule 3 of the IP Act as well as complying with Council's *Privacy Policy* and other relevant legislation and documents.

[13] *Information Privacy and Other Legislation Amendment Act 2023* (Qld), s 50.

Chief Executive Officer (CEO) and Executive Team

The CEO and Executive Team will endorse Council's *Privacy Policy* for Council adoption and provide leadership and commitment in complying with the IP Act and the associated QPPs contained in Schedule 3 of the IP Act, as well as complying with Council's *Privacy Policy* and other relevant legislation and documents.

Council employees

When dealing with personal information, Council employees will comply with the IP Act and associated QPPs contained in Schedule 3 of the IP Act as well as complying with Council's *Privacy Policy* and any other relevant legislation and documents.

Council employees will immediately notify their Supervisor / Manager / Director if they suspect a privacy breach has occurred so Council can manage the risk in accordance with legislative, policy and procedural requirements.

Contractors and service providers of Council

Council occasionally enters into contracts with external bodies for the supply of goods and services. Some of these contracts require the disclosure of personal information to third parties, or the collection of personal information by third parties on behalf of Council. Through the execution of contracts, Council will mandate that contractors and service providers comply with the same rules and regulations as Council, including Council's *Privacy Policy*.

Governance Branch

The Governance Branch will periodically review Council's *Privacy Policy*, educate employees on the application of the Policy, provide advice to Council employees on privacy related matters, participate as a member of the Data Breach Response Team and administer and investigate privacy complaints for Council.

ICT Branch

The ICT Branch will work closely with the Governance Branch to ensure our high-risk technology projects are compliant with privacy laws, provide technical ICT support and advice where required, and participate as a member of the Data Breach Response Team.

Privacy complainant

Complainants are entitled to a prompt response to their privacy complaint within statutory timeframes (45 business days) and to be kept informed of the progress and outcome of the complaints process. Furthermore, Complainants can expect that the confidentiality of their personal information shall be maintained (where possible within the law) and a thorough and objective investigation or review of their complaint.

DEFINITIONS

Term	Meaning
Complainant	For a privacy complaint, means the person who makes the complaint.
Consent	Voluntary agreement to some act, practice or purpose.
Disclosure	The release of personal information as defined in section 23(1) of the IP Act.

Term	Meaning
Personal information	Information or an opinion about an identified individual or an individual who is reasonable identifiable from the information or opinion, whether true or not, and whether recorded in a material form or not.
Privacy complaint	A complaint made by an individual about an agency that has breached its obligations under the IP Act and has failed to comply with the QPPs or an approval under section 157 of the IP Act.
Privacy principles	The Queensland Privacy Principles as outlined in Schedule 3 of the *Information Privacy Act 2009*.

RELEVANT LEGISLATION

- *Information Privacy Act 2009*
- *Information Privacy Regulation 2009*
- *Information Privacy and Other Legislation Amendment Act 2023*
- *Local Government Act 2009*
- *Local Government Regulation 2012*
- *Human Rights Act 2019*
- *Public Records Act 2023*
- *Right to Information Act 2009*
- *Right to Information Regulation 2009*

HUMAN RIGHTS STATEMENT

In developing this Policy, the subject matter has been considered in accordance with the requirements of the Queensland *Human Rights Act 2019*. It is considered that the subject matter does not conflict with any human rights, including the right to privacy and freedom of expression, and supports a human rights approach to decision making by Council.
Council representatives will endeavour to act and make decisions under this Policy in a manner that is compatible with human rights. In particular, representatives will endeavour to:

(a) identify relevant human rights which may be affected by the action or decision,
(b) give proper consideration to the impact of its actions and decisions on human rights, and,
(c) ensure that any conduct or decision by Council which limits an individual's human rights is reasonable and justifiable.

This policy should be read in conjunction with Council's *Human Rights Policy*.

Version control:

Version	Reason / Trigger	Change (Y/N)	Endorsed / Reviewed by	Date
1.0	New	Y	CEO	23/06/2014
2.0	Review – legislative reforms	Y	Council / Executive Team	19/12/2024

APPENDIX A – DATA BREACH RESPONSE PLAN

INTRODUCTION

This data breach response plan (Response Plan) sets out procedures and clear lines of authority for Council employees in the event that Council experiences a data breach (or suspects that a data breach has occurred). Council has prepared and published this policy about how it will respond to a data breach, including a suspected eligible data breach, in accordance with legislative requirements.[14]

This Response Plan is intended to enable Council to contain, assess and respond to breaches quickly, to help mitigate potential harm to affected individuals and to comply with the IP Act. Our actions in the first 24 hours after discovering a data breach are crucial to the success of our response.

The Response Plan sets out details for Council employees in the event of a data breach, clarifies key roles and responsibilities, and documents processes to assist Council to respond to a data breach.

Key Definitions

Data Breach –

A data breach of Council, means either of the following in relation to information held by Council:

a) unauthorised access to, or unauthorised disclosure of, the information,
b) the loss of the information in circumstances where unauthorised access to, or unauthorised disclosure of, the information is likely to occur.[15]

Therefore, a data breach is when data is shared, disclosed, or accessed without authorisation, or is lost. An organisation that is the victim of a data breach does not always know, at the time it detects or is told of the breach, what data has been compromised. The organisation may have to investigate to determine whether personal information has been released or accessed without authorisation.[16] For example, data breaches include loss or theft of physical devices, misconfiguration or overprovisioning of access to system, social engineering and hacking.

Eligible Data Breach –

Furthermore, an eligible data breach occurs in relation to personal information if both of the following factors apply:

a) the data breach involves unauthorised access to, or unauthorised disclosure of, the personal information,
b) the access or disclosure is likely to result in serious harm to an individual to whom the personal information relates, having regard to the matters stated below:
    i. the kind of personal information accessed, disclosed or lost,
    ii. the sensitivity of the personal information, and
    iii. whether the personal information is protected by 1 or more security measures, and
    iv. if the personal information is protected by 1 or more security measures – the likelihood that any of those security measures could be overcome, and
    v. the persons, or the kinds of persons, who have obtained, or who could obtain, the personal information, and
    vi. the nature of the harm likely to result from the data breach, and

[14] *Information Privacy and Other Legislation Amendment Act 2023* (Qld), s 73.
[15] *Information Privacy and Other Legislation Amendment Act 2023* (Qld), schedule 5.
[16] Office of the Information Commissioner, *Report No. 4 to the Queensland Legislative Assembly for 2022-23*, p. 7.

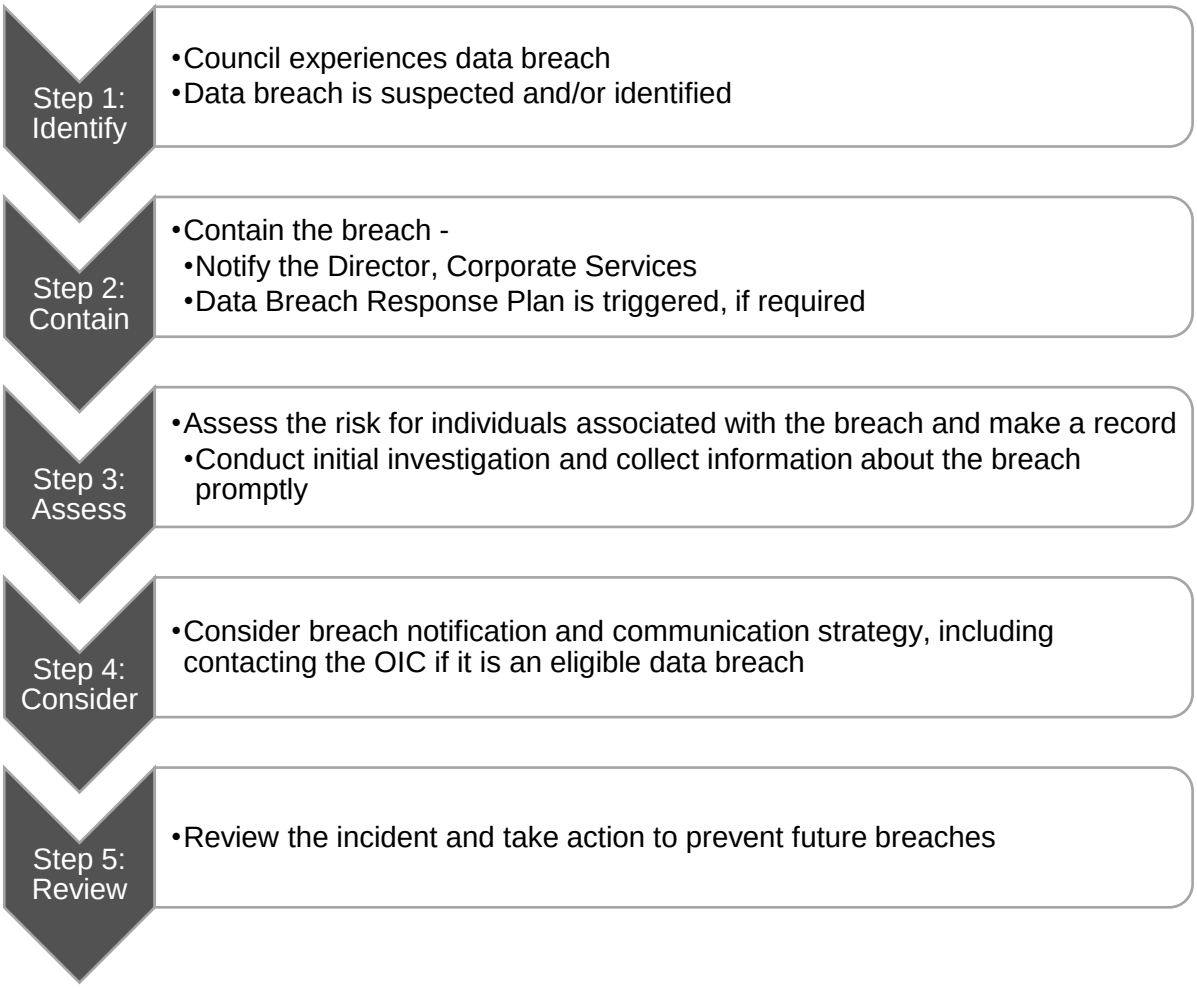
vii. any other relevant matter.[17]

Privacy Breach –

A privacy breach can happen when personal information is accessed, used, or disclosed without authorisation or is lost, or otherwise dealt with in a way that would not comply with the Act. This may result from a data breach. However, a privacy breach is not necessarily a data breach. For example, a privacy breach can occur if an organisation does not give sufficient notice to a person about collecting their personal information.[18] Other examples include a Council employee misusing personal information located in a Council database or sending information in an email to unauthorised recipients.

DATA BREACH RESPONSE STRATEGY

Council's Response Plan strategy is summarised into key steps that Council will undertake to manage and respond to a data breach.



[17] *Information Privacy and Other Legislation Amendment Act 2023* (Qld), s 47.
[18] Ibid.,

Step 1: Identify the breach

A suspected data breach may be discovered by Council employees, or a contractor, or Council may be otherwise alerted (for example, by a member of the public or the media).

If a Council employee becomes aware of, or are notified of a data breach, they will record and advise management of the following:

a) the time and date the suspected breach was discovered,
b) the type of personal information involved,
c) the cause and extent of the breach, and
d) the context of the affected information and the breach.

The public or another agency / external entity can immediately report an actual or suspected data breach directly to Council via the following contact details:

Website: www.noosa.qld.gov.au/about-council/contact-council
Phone: (07) 5329 6500
Email: mail@noosa.qld.gov.au

Step 2: Contain and manage the breach

- Council employees to notify the Director, Corporate Services ('Director') who may convene the Data Breach Response Team. *Note - the Director may delegate part of their involvement to the ICT Manager for immediate response.*
- The Director should coordinate any immediate action required to contain the breach. Depending on the breach, this may include contacting unauthorised recipients requesting them to delete the email or requesting information be removed from a website.
- Immediately contain the breach:
    - ICT Branch to implement any immediate technical / software solutions to reduce risk.
    - Director / ICT Branch to contact external ICT providers to support containment through immediate technology solutions.
    - Director / ICT Branch / Governance Branch to contact Council's insurer and cyber incident response platform for containment support, if required.
- Director to consider whether Council needs other expertise support.
- Director to inform the CEO as soon as possible and Council's insurer; provide ongoing updates on key developments in this stage.
- Director to notify the Governance Branch about the data breach after coordinating any immediate action.
- Director to ensure evidence is preserved that may be valuable in determining the cause of the breach or allowing the Council to take appropriate corrective action.
- In consultation with the CEO, the Director is to consider a communications or media strategy to manage public expectations at this stage. The Director and CEO may consult with Council's Communications and Community Engagement Manager and Legal Counsel.

Step 3: Assess the risks for individuals associated with the breach

- Governance Branch to determine whether the breach constitutes a Mandatory Notifiable Data Breach. The team should initially assess the data breach, which may involve asking for further information or documentation from the Director who reported the breach or the Council employee who identified the breach.
- Governance Branch to conduct an initial investigation and collect the following information about the breach that will form part of that assessment:

  - the date, time, duration, and location of the breach,
  - the type of personal information involved in the breach,
  - how the breach was discovered and by whom,
  - the cause and extent of the breach,
  - a list of the affected individuals, or possible affected individuals,
  - the risk of serious harm to the affected individuals, and
  - the risk of other harm.
- Following the assessment, the Director will decide whether any further action is required to contain the breach, including but not limited to:
  - Instructing ICT Branch to activate the Cyber Incident Response Plan and/or ICT Business Continuity Plan.
  - Alerting Building and Facilities security if necessary.
  - Advising Records systems administrators.
  - Advising any other system administrators that may be impacted.
- The Director and/or Governance Branch need to keep appropriate records of the suspected breach and actions of the Data Breach Response team, including the steps taken to rectify the situation and the decisions made. The Executive Assistant to the CEO may assist with such record-keeping duties, including minutes and action logs.

Step 4: Consider breach notification and communication strategy

- On each occasion of a data breach, the Director must consider whether to convene the Data Breach Response Team.
  - Some data breaches may be comparatively minor, and able to be dealt with easily without action from the response team. For example, a Council employee may, as a result of human error, send an email containing personal information to the wrong recipient. Depending on the sensitivity of the contents of the email, if the email can be successfully recalled, or if the officer can contact the recipient and obtain an assurance that the recipient has deleted the email, it may be that there is no utility in escalating the issue to the Data Breach Response Team.
- The Director needs to:
  - Determine who needs to be made aware of the breach (internally, and potentially externally) at this stage. This may include notifying Council's insurer, law enforcement, other organisations, and external regulators.
  - Determine whether and how to notify affected individuals as soon as reasonably practicable.
- As part of Council's communication strategy and response, the Director and CEO may consult with Council's Communications and Community Engagement Manager and Legal Counsel.

<u>Eligible Data Breach:</u>

- The Governance Manager and Branch need to:
  - Determine whether the breach triggers the requirements of the IP Act – whether the breach is likely to be considered an eligible data breach that needs to be notified to the OIC. Questions to assist in the determination include:
    - Whether multiple individuals are affected by the breach or suspected breach
    - Is there (or may there be) a real risk of serious harm to any affected individuals?
    - Does the breach or suspected breach indicate a systemic problem in Council processes or procedures?
    - Could there be media or stakeholder attention as a result of the breach or suspected breach?
  - If an eligible data breach has occurred or is taken to have occurred, the Governance Branch will inform the OIC immediately using their approved reporting form.

    - Further information may be provided by the Governance Branch to the OIC, if required.
- The Governance Branch will inform Council's insurer immediately of the breach via phone/email.
- In parallel, the ICT Manager will contact Council's ICT cyber incident response platform to trigger notification and support.
- On behalf of the Director, the ICT Branch may alert all staff to key communication messages via appropriate internal mechanisms.
- In consultation with the Director, Corporate Services, Communications and Community Engagement Manager and legal counsel, the CEO will determine whether a media announcement / communication is required.
- Affected individuals, or their authorised representative, will be notified by Council as soon as reasonably practicable. This may occur via formal correspondence, email, or phone.

Where a data breach is not an eligible data breach:

- Council will still consider notifying the OIC for transparency and to reduce risk if it is deemed appropriate.
- Council will still consider notifying individuals and organisations about the breach, depending upon the type of information involved, the risk of harm, repeated and/or systemic issues and the ability of an individual or organisation to take steps to avoid or remedy harm.
- The Governance Branch will still notify the insurer, if it is deemed to be a high-risk incident, in order to alert the local government sector to emerging risks.

Step 5: Review the incident and take action to prevent future breaches

- The Data Breach Response Team will undertake a post breach review and draft a report outlining:
    a) the cause of the breach,
    b) implementation of any strategies to identify and address any weaknesses in data handling that may have contributed to the breach,
    c) revising employee training practices, if necessary,
    d) considering the option of a future audit to reduce risks,
    e) consider whether the make-up of the response team needs other expertise
    f) changes made to policies and procedures, if necessary, and
    g) the effectiveness of this data breach response plan.
- The Report will be presented to the CEO, including outcomes and recommendations.
- The Data Breach Response Team should also consider other relevant documents, including ICT Cyber Incident Response Plan and Business Continuity Plan.
- The Director, Corporate Services will report the results to Council's Executive Team and Council's Audit and Risk Committee.

DATA BREACH RESPONSE TEAM

Membership of the Data Breach Response Team comprises of the following standing members:

- Chief Executive Officer
- Director, Corporate Services
- ICT Manager
- Governance Manager
- Communications and Community Engagement Manager
- People & Culture Manager, if required
- Legal Counsel
- ICT Operations Coordinator
- Records Supervisor

- Executive Assistant to the CEO

The Data Breach Response Team may draw on the expertise of other internal and external roles and functions in order to respond effectively to the breach. Outside assistance will be sought from experts on a case-by-case basis depending on the nature of the breach.

ROLES AND RESPONSIBILITIES

The following key roles and responsibilities are outlined to support the Data Breach Response Plan.

Chief Executive Officer (CEO)
Overall authority and accountability for the data breach response, on behalf of Council, rests with the CEO. The CEO will respond and report to the Executive Team and Councillors. If required, the CEO will also issue any communications / media releases, on behalf of Council, in relation to the data breach.

Director Corporate Services
Executive Team leader who has authority and is responsible for leading the Data Breach Response Team and reporting to Executive management and the CEO.

ICT Manager
To provide information and communication technology support / forensic support and response, which includes helping to establish the cause and impact of the data breach that involved ICT systems. This may require liaising with Council's insurer.

Governance Manager
To provide privacy and risk management expertise to the team and undertake relevant functions, such as conducting the investigation. The Governance Manager will report any eligible data breaches to the OIC in accordance with legislative requirements.

Communications and Community Engagement Manager
To provide media and communications expertise to the CEO, Director, and Data Breach Response Team. This may include preparing and issuing approved media announcements and statements to the community via various platforms.

People and Culture Manager
To provide human resource expertise and support to the team if the breach was due to the actions of a Council employee.

Legal Counsel
To identify legal obligations and provide legal advice to Council, if required.

ICT Operations Coordinator
To assist in reviewing security monitoring controls related to the breach (e.g., access, authentication, encryption, audit logs), to provide ICT and forensic support and to liaise with Council's insurer of any breaches.

Records Supervisor
To provide information and records management expertise and advice on recording the response to the data breach.

Executive Assistant to the CEO
To provide administrative and reporting assistance to the Data Breach Response Team.

REVIEW AND TESTING THE PLAN

This Data Breach Response Plan will be reviewed comprehensively once per Council term (every four years) or as required from time to time. Regular desktop reviews and updates will occur at least annually throughout the term to ensure currency.

Members of the Data Breach Response Team will regularly test the Response as part of Council's Business Continuity Plan testing schedule, to ensure that it is operationally effective, up to date and considers the changeability of the external threat environment. Regular testing will allow for the checking of response processes, such as contacts, approval process and reporting lines to ensure they are current.