Policy title	Data Breach Policy
Policy category	Operational (internal)
Responsible manager(s)	General Manager
Contact officer(s)	Corporate Manager, Governance and Information
Directorate	Finance and Corporate Services
Approval date	06 December 2023
Outcome area	5. Our engaged community with progressive leadership
Strategy	5.2 Proactive, responsive and strategic leadership
Delivery program link	5.2.2 Implement effective governance and long-term planning
Operational program link	5.2.2.1 Assist the Council in meeting its statutory obligations and roles

Purpose

To provide guidance to Eurobodalla Shire Council staff in responding to a breach of Council held data, especially personal information.

Part 6A of the *Privacy and Personal Information Protection Act 1998 (NSW)* (PPIP Act) establishes the NSW Mandatory Notification of Data Breach (MNDB) scheme.

The MNDB scheme requires every NSW public sector agency bound by the PPIP Act to notify the Privacy Commissioner and affected individuals of eligible data breaches.

Under the scheme, public sector agencies are required to prepare and publish a Data Breach Policy (DBP) for managing such breaches.

All public sector agencies as defined in section 3 of the PPIP Act are required to prepare and publish a DBP. This includes all NSW agencies and departments, statutory authorities, local councils, state-owned corporations, Ministers' offices, and some universities.

This DBP outlines Council's overall strategy for managing data breaches from start to finish.

Having a clear and well-defined DBP enables Council to:

- Prepare for, evaluate, respond to and report on data breaches at the appropriate level and in a timely fashion.
- Mitigate potential harm to affected individuals and the agency itself.
- Meet compliance obligations under the PPIP Act.

This Policy aims to:

- Protect important business assets (data) including personal and health information and Council's reputation.
- Support Council's legal obligations under the *Privacy and Personal Information Protection Act 1998* (NSW), *Health Records and Information Privacy Act 2002* (NSW) and requirements governed by the Federal Office of the Australian Information Commissioner (OAIC) and the NSW Information and Privacy Commission (IPC) with respect to handling personal and health information.
- Ensure effective breach management, including notification where warranted.
- Assist Council in avoiding or reducing possible harm to both the affected individuals/ organisations and the Council and may prevent future breaches.
- Detail the principles, goals and responsibilities associated with mandatory data breach notification and data response planning.

Policy details

1	**Application** This Policy applies to all persons employed at Council, including employees, councillors, contractors, students, volunteers, and agency personnel. This Policy also applies to external organisations and their personnel who have been granted access to Council Information & Technology (I&T) infrastructure, services, and data. The scope of the Policy includes Council data held in any format or medium (paper based or electronic). The Policy does not apply to information or data that has been classified as public.
2	**Legislation** This DBP ensures Eurobodalla Shire Council's compliance with Part 6A of the *Privacy and Personal Information Protection Act 1998 (NSW)* (PPIP Act). This policy has been prepared using the NSW Information and Privacy Commission (IPC) *Guide to Preparing a Data Breach Policy* (May 2023). It intends to meet the NSW Privacy Commissioner's expectations in relation to preparing a DBP to ensure Council's compliance with section 59ZC of the PPIP Act.
3	**Background and terminology**
3.1	**What is an eligible data breach?** An 'eligible data breach' occurs when: 1. There is an unauthorised access to, or unauthorised disclosure of, personal information held by a public sector agency or there is a loss of personal information held by a public sector agency in circumstances that are likely to result in unauthorised access to, or unauthorised disclosure of, the information, and 2. A reasonable person would conclude that the access or disclosure of the information would be likely to result in serious harm to an individual to whom the information relates. **Data Breach means:** An incident where there has been unauthorised access to, unauthorised disclosure of, or loss of, personal information held by (or on behalf of) Eurobodalla Shire Council. **Serious Harm means**: Serious physical, psychological, emotional, financial or reputational harm. This could include risk to individuals' safety, risk of identity theft, financial loss to an individual. Breaches can occur between agencies, within an agency and external to an agency. The MNDB scheme applies to breaches of 'personal information' as defined in section 4 of the PPIP Act; meaning information or an opinion about an individual whose identity is apparent or can reasonably be ascertained from the information or opinion. The MNDB scheme also applies to 'health information,' defined in section 6 of the *Health Records and Information Privacy Act 2002* (HRIP Act), covering personal information about an individual's physical or mental health, disability, and information connected to the provision of a health service.

	The scheme does not apply to data breaches that do not involve personal information or health information, or to breaches that are not likely to result in serious harm to an individual. Where the scheme does not apply, Council is not required to notify individuals or the Information Commissioner (IC) but should still take action to respond to the breach. Council may still provide voluntary notification to individuals where appropriate.
3.2	**What is a DBP?** A DBP is a documented policy or plan setting out how Council will respond to a data breach. Agencies are required to draft a DBP under section 59ZD of the PPIP Act. This DBP establishes the roles and responsibilities of Council staff in relation to managing a breach, and the steps that Council will follow when a breach occurs. Council is required to ensure its DBP is publicly accessible. This DBP will be published on Council's website. A link to the DBP will also be available on the Council intranet to ensure staff know how to access the policy.
3.3	**Why is a DBP necessary?** Depending on the size and nature of a data breach, the consequences for individuals can be significant. They can give rise to a range of actual or potential harm to individuals. These consequences can include financial fraud, identity theft, damage to reputation and even violence. Data breaches can also have serious consequences for government agencies. A breach may create risk through the disclosure of sensitive information, or otherwise impact an agency's reputation, finances, interests, or operations. Ultimately, data breaches can lead to a loss of trust and confidence in an agency and the services it provides. Responding quickly when a breach occurs can substantially reduce its impact on affected individuals, reduce the costs to agencies of dealing with a breach and reduce the potential reputational damage that can result. For these reasons, it is important that Council has a documented and operationalised plan or framework for quickly and effectively responding to and managing data breaches.
3.4	**Why must Council publish their DBP?** Making a DBP publicly accessible enhances transparency and ensures Council remains accountable for the way it responds to data breaches. It also enhances public trust and confidence in government and the services it provides.

3.5	**What if Council is also required to notify the Commonwealth regulator?** In some cases, Council will have notification obligations under both the MNDB scheme and under the Commonwealth Notifiable Data Breach (NDB) scheme. For example, a data breach at a NSW public sector agency that involves Tax File Numbers and is likely to result in serious harm would be reportable to both the Office of the Australian Information Commissioner (OAIC) under the Commonwealth NDB scheme, and the NSW Privacy Commissioner under the MNDB scheme. The MNDB scheme has been designed to be consistent with and adopt, as far as possible, key features of the Commonwealth NDB scheme. For example, the MNDB scheme adopts the same thresholds for assessing and notifying data breaches so that agencies can meet both requirements with a single process.
4	**What is included in this DBP?** Having a clear and well-defined DBP enables Council to: • Prepare for, evaluate, respond to and report on data breaches at the appropriate level and in a timely fashion. • Mitigate potential harm to affected individuals and Council. • Meet compliance obligations under the PPIP Act. This DBP outlines Council's overall strategy for managing data breaches from start to finish, including the following: 1. How Council has prepared for a data breach. 2. A clear description of what constitutes a breach. 3. Strategy for containing, assessing, and managing eligible data breaches. 4. Roles and responsibilities of staff members. 5. Record keeping requirements. 6. Post-breach review and evaluation.
4.1	**How Council has prepared for a data breach** A DBP should provide a high-level outline of the steps that Council has taken to prepare for a data breach, and how these fit within the Council's broader systems, policies and procedures (such as cyber response, broader incident or emergency management processes, communications strategies and risk management frameworks). This DBP covers key controls, systems, and processes that Council has in place to promptly identify actual or suspected data breaches, and to ensure they are effectively managed.
4.1.1	**Training and awareness** Most data breaches, both in Australia and internationally, involve a human element (either through direct human error or cyber-attacks that rely on a human compromise). Building a well-trained and aware workforce is a strong front-line defence against breaches and other privacy risks. Council's approach to staff training and awareness is: • Training and awareness around identifying, responding to, and managing data breaches. • Enhancing staff awareness of privacy and current threat trends. • Mandatory cyber security training for all staff and annual refresher training**.**

4.1.2	**Processes for identifying and reporting breaches** The quicker Council can detect a data breach, the better chance it may be contained, and potential harms mitigated through prompt action. Council has the following processes in place to assist in preventing data breaches: • All suspicious activities are reported IT helpdesk for investigation. • Security information and event management system for log file collection, incident correlation and alerting. • Firewall logs are monitored daily for suspicious activity. • Microsoft Security/365 monitors for data leakage via email and OneDrive. • Ongoing staff training and cyber security skills development.
4.1.3	**Appropriate provisions in contracts / other collaborations** Council is often required to outsource functions to external service providers or another agency (for example, for Strategic Planning). These relationships are usually covered by legally binding contracts, memorandums of understanding or non-disclosure agreements. To ensure Council meet their obligations under the PPIP Act, these agreements often include provisions in relation to the management and notification of data breaches. Council's approach to managing these collaborations and the contractual controls in place for ensuring external stakeholders comply with relevant privacy requirements are via contract provisions and not sharing personal information with third parties via email or other unsecured means.
4.1.4	**Schedule for testing and updating the DBP** A DBP will only be effective if it is current, appropriately targeted and operationalised. As both the external threat environment, and Council's internal makeup and functions, are continuously developing and changing, a DBP should be regularly reviewed to ensure it remains fit for purpose. Regular testing of the data breach response process is the best way to ensure all relevant staff understand their roles and responsibilities, and to check that the details of the response process (contact numbers, reporting lines, approval processes, etc.) are up to date. Testing the DBP could involve the development of a hypothetical or test incident and a review of the way agency personnel manage the event. Council's DBP will be reviewed, tested, and updated annually.
4.1.5	**Alignment with other policies** This DBP is aligned with existing policies, procedures, and capabilities including Council's Cyber Security Response Plan and Privacy Management Plan, including cross references where relevant. Further, Council has developed a Cyber Incident Response Plan (CIRP) that addresses data beaches associated with ICT systems. The CIRP contains response and communication plans around suspected data breaches.

4.2	**What a data breach is and how to identify one** To assist staff and others in identifying data breaches, this DBP includes a clear description of what a data breach is and how a data breach may occur. **Data Breach means:** An incident in which there has been unauthorised access to, unauthorised disclosure of, or loss of, personal information held by (or on behalf of) Council. Consistent with the definition of 'eligible data breach' in section 59D of the PPIP Act, a data breach may involve unauthorised access, unauthorised disclosure, or loss of personal information. A data breach may be deliberate or accidental and may occur by a range of different means or channels, including but not limited to, loss or theft of physical devices, misconfiguration or over-provisioning of access to sensitive systems, inadvertent disclosure, social engineering or hacking. Examples of a data breach are as follows. • **Business email compromise (BEC)** - A user receives an email with a link to a document on an online file sharing platform such as OneDrive. The user opens the link and a PDF document with an embedded form resembling the Microsoft login page is presented. The user enters their ESC credentials, and these credentials are collected and sent to the malicious actor. The cyber criminals now have full access to the user's mailbox, OneDrive, SharePoint, and potentially Tech1/CIAnywhere if the user is in an exempted multi-factor authentication category. • **Improper use and disposal or personal equipment** - A user has been working remotely and using their own personal PC for convenience. They have signed into OneDrive on the PC and their files are being sync'd to the local computer. The staff member then purchases a new PC and sells the old one on Gumtree without erasing the hard drive. The purchaser now has offline access to all of the files in the user's OneDrive folder. Each data breach should be assessed on a case-by-case basis and no template response can be applied in all cases.
4.3	**Plan for managing data breaches** This DBP outlines the steps Council will take to respond to a reported, suspected or confirmed data breach.
4.3.1	**Plan to triage, contain, assess, notify, prevent** The quicker Council can detect a data breach, the better the chance that it may be contained, and potential harms mitigated through prompt action. 1) How to report: in all cases, staff must report a suspected data beach immediately to the Chief Information Officer and the Privacy Officer. 2) Contain the breach: all necessary steps must be taken to contain the breach and minimise any resulting damage. For example, recover the personal information, shut down the system that has been breached, suspend the activity that leads to the breach, revoke or change access codes or passwords. If a third party is in possession of the data and declines to return it, it may be

	necessary for Council to seek advice from Cyber Security NSW, legal advice or other advice on what action can be taken to recover data. 3) Assessment – Chief Information Officer and Privacy Officer should conduct preliminary fact-finding about the breach, including type of data (e.g. check if Tax File Numbers were involved), cause, risk of spread and option to mitigate. Make a preliminary assessment of the risk posed by the breach, as Low, Medium or High according to the criteria below. **Low risk data breach:** a loss or exposure of aggregated data only, or of individual level data in circumstances where it is reasonably believed that no harm could occur (e.g. paper files are left behind in a meeting but quickly retrieved). **Medium risk data breach:** a loss or exposure of personal information where it is reasonably believed that the third-party recipient does not have a malicious intent, and that the data is somewhat protected (e.g. laptop with encrypted data left on a bus). **High risk data breach:** it is reasonably believed that the data breach is likely to result in serious harm to one or more of the individuals to whom the information relates (e.g. external hackers breach Council's firewall and copy valuable customer data). 4) Notify: Council recognises that notification to individuals/organisations affected by a data breach can assist in mitigating any damage for those affected individuals/organisations. Notification demonstrates a commitment to open and transparent governance. Accordingly, Council adopts a relatively low threshold in considering whether to notify individuals of the release or risk to the security of their personal information and will generally make such a notification. Council will also have regard to the impact upon individuals in recognition of the need to balance the harm and distress caused through notification against the potential harm that may result from the breach. There are occasions where notification can be counterproductive. For example, information collected may be less sensitive and notifying individuals about a privacy breach that is unlikely to result in an adverse outcome for the individual may cause unnecessary anxiety and de-sensitise individuals to a significant privacy breach. 5) Prevent: Council will further investigate the circumstances of the breach to determine all relevant causes and consider what short-term measures could be taken to prevent any reoccurrence. For High Risk or Medium Risk breaches the Privacy Officer must submit a report within 10 working days to the General Manager outlining the organisational response and mitigation plan.
4.3.2	**3.3.4 How to notify individuals.** There are three options for notifying individuals at risk of serious harm, depending on what is applicable: • Directly notify only those individuals at risk of serious harm, or • Directly notify all individuals whose data was breached, or • Publicise the statement more broadly. Where it is possible to identify and contact only those individuals at risk of serious harm, Council must directly notify those individuals. Council might also publish the notification more broadly, including on its website. Where it is not possible to identify which individuals might be at risk of serious harm, but it is possible for Council to directly contact all individuals whose data was breached, then Council will directly notify all individuals whose data was breached. Council might also publish the notification more broadly, including on its website.

	Where it is not possible to identify which individuals might be at risk of serious harm, and it is not practical to directly contact all individuals whose data was breached (for example, if Council don't have up-to-date contact details for old customers), then Council must publish on its website. Council can also consider other methods of communication such as social media.
4.3.3	**Other obligations including external engagement or reporting** Council may be required by contract or by other laws or administrative arrangements to take specific steps in response to a data breach. These may include taking specific containment or remediation steps or engaging with or notifying external stakeholders (in addition to the Privacy Commissioner), where a data breach occurs. Depending on the circumstances of the data breach and the categories of data involved, Council may need to notify or engage with: • NSW Police Force • Department of Customer Service • Cyber Security NSW • The Office of the Australian Information Commissioner • Australian Federal Police • The Australian Taxation Office • The Australian Digital Health Authority • The Department of Health • The Office of the Government Chief Information Security Officer • The Australian Cyber Security Centre • Any third-party organisations or agencies whose data may be affected • Financial services providers • Professional associations, regulatory bodies or insurers • Foreign regulatory agencies. If the breach involves cybercrime, contact the Australian Cybercrime Online Reporting Network which will coordinate a police response. For other types of criminal activity (e.g. theft), contact the local police. For other cybersecurity incidents requiring support or assistance, contact Cyber Security NSW.

4.3.4	**Capability, expertise and resourcing** To be effective, the strategies outlined above must be able to be quickly and effectively implemented and actioned. However, this depends on having staff with the relevant skillsets available to deal with the breach. Relevant expertise will be gathered from inhouse subject matter experts, management, communications and where required external professionals. Initial investigation of the breach will assist in determining the skills and resources required. Support and/or guidance from leading agencies such as Cyber Security NSW, Information and Privacy Commission NSW and the like, may be sourced when and where required.
4.4	**Roles and responsibilities** **General Manager** • Ensure Council has systems in place to comply with the MNDB scheme. • Review and approve actions and recommendations in data breach reports. • Demonstrate to the affected individuals and broader public that Council views the protection of personal information as an important and serious matter. **Governance and Information Officer (Privacy Officer)** • On being alerted to a data breach, immediately notify the General Manager and the Chief Information Officer. • Review proposed actions and recommendations in reports prepared by the Chief Information Officer and provide to the General Manager for approval. • If the breach relates to any area other than Information Technology or Information Management, investigate the breach in a timely and effective manner and prepared a report and provide to the General Manager for approval. • Implementation of proposed actions and recommendation, including and follow up with other staff. • Notify the Privacy Commissioner if the breach results (or could result) in serious harm to an individual(s) or if the data breach resulted in personal information being disclosed and there are risks to the privacy of individuals. • Constitute the Data Breach Response Team, if required. **Chief Information Officer** • If the breach relates to Information Technology or Digital Information Management, immediately notify the General Manager and the Privacy Officer. • Investigate the breach in a timely and effective manner and prepare a report to the General Manager. • Implement any proposed actions and recommendations and inform the General Manager of any progress. **Corporate Manager Coordination and Communication** • Authorise communication to individuals affected by data breaches. **Data Breach Response Team** • Review the Governance and Information Officer's and Chief Information Officer's initial assessment of the data breach. • Establish roles within the team based on subject matter expertise (could include legal, communications, cybersecurity, human resources, key operational staff). • Delineation of responsibilities for dealing with relevant elements of a breach within the team.

	• Investigate the breach using the five-step process outlined in 4.3.1 of this policy. • Determine whether Council's Business Continuity Plan needs to invoked, particularly if IT systems have to be shut down. **Staff** It is everyone's responsibility to be aware of this policy and to report suspected data breaches as soon as possible. Even if you have contained the breach (for example, retrieved a stolen laptop or lost hard-copy files) you must still tell the Privacy Officer. The Privacy Officer will assess any residual risk, and they can also consider whether further action is needed to avoid a similar occurrence.
4.5	**Record-keeping** Appropriate records must be maintained to provide evidence of how suspected breaches are managed, including those not escalated to the response team or notified to the Privacy Commissioner. Tracking data breaches allows us to monitor, analyse and review the type and severity of suspected breaches along with the effectiveness of the response methods. This may help to identify and remedy weaknesses in security or processes that are prone to error. Council will meet its record keeping obligations under the PPIP Act to: • Maintain and publish (on its website) a public notification register for any notifications given under section 59N(2). (s 59P) • Establish and maintain an internal register for eligible data breaches. (s 59ZE) • Publishing Council's Privacy Management Plan and DBP on its website.
4.6	**Post-breach review and evaluation** A Date Breach Response Report will be prepared. This report requires the responsible officer to report on what has been done to prevent a recurrence of the data breach and any changes recommended to Council protocols, controls, policies and procedures or staff training etc. Data Breach Response Report will include: • • A strategy to identify and remediate any processes or weaknesses in data handing that may have contributed to the breach. • • A post-response assessment of how the agency responded to the breach and the effectiveness of the DBP. Understanding what went wrong, how issues were addressed and whether changes were needed to processes and procedures following a breach will mitigate future risks and are key to ensuring Council continue to proactively manage data breaches in line with regulator and community expectations.

Implementation

Requirements		Responsibility
1	**Staff** Under supervision, applicable Council staff will be responsible for ensuring that Council codes and procedures are implemented appropriately within their work area, after they have received relevant training to do so.	Council Officers
2	**Concerns about this Policy** Concerns communicated to Council in relation to this policy will be recorded on Council's records system and handled in accordance with Council's relevant policy. These records will be used to analyse the history of concerns and help determine follow up actions.	Council Officers
3	**Complaints about this code** Complaints received in relation to this policy will be lodged with the Public Officer and handled in accordance with Council's Complaints Policy.	Public Officer
7	**Consultation** Any consultation deemed necessary will occur as required with key stakeholders, that may include the community, other agencies, legislative bodies, relevant legislation, and industry guidelines. This policy will not be publicly exhibited for the community input prior to adoption as it is a policy for Council staff to follow if they detect a data breach.	As applicable

Review

This policy will be reviewed and updated as necessary if legislation or Council policy changes require it; or Council's functions, structure or activities change; or when technological advances or new systems change the way that Council manages data breaches.

Reviews of the effectiveness of this code could include the following:

Performance indicator	Data source(s)
Concerns or complaints registered	Council records
Customer Feedback/ Survey Responses	Surveys
Internal or external review	Audit
Number of Data Breaches and measure taken	Internal reporting
Any other relevant performance indicator	As applicable

Governance

This policy should be read in conjunction with any related legislation, codes of practice, relevant internal policies, and guidelines.

Related legislation and policies

Name	Link
Privacy and Information Protection Policy	https://www.esc.nsw.gov.au/__data/assets/pdf_file/0003/138603/ECM_4625938_Privacy-and-Information-Protection-Policy.pdf
Privacy Management Plan	https://www.esc.nsw.gov.au/__data/assets/pdf_file/0010/138736/Privacy-Management-Plan-2020.pdf
Complaints Policy	https://www.esc.nsw.gov.au/__data/assets/pdf_file/0008/138563/ECM_4625898_Complaints-Policy.pdf
Local Government Act 1993	www.legislation.nsw.gov.au/maintop/view/inforce/act+30+1993+cd+0+N
Government Information (Public Access) Act 2009	https://legislation.nsw.gov.au/view/html/inforce/current/act-2009-052
Health Records and Information Act 2002	https://legislation.nsw.gov.au/view/html/inforce/current/act-2002-071
Privacy and Personal Information Protection Act 1998	https://legislation.nsw.gov.au/view/html/inforce/current/act-1998-133

Related external references

Name	Link
Information and Privacy Commission	www.ipc.nsw.gov.au
Guide to managing data breaches in accordance with the PPIP Act	https://www.ipc.nsw.gov.au/guide-mandatory-notification-data-breach-scheme-guide-managing-data-breaches-accordance-ppip-act
Guide to preparing a data breach policy	https://www.ipc.nsw.gov.au/guide-mandatory-notification-data-breach-scheme-guide-managing-data-breaches-accordance-ppip-act

Definitions

Word/Term	Definition
Data Breach	An incident where there has been unauthorised access to, unauthorised disclosure of, or loss of, personal information held by (or on behalf of) Eurobodalla Shire Council.
Serious Harm	Serious physical, psychological, emotional, financial or reputational harm. This could include risk to individuals' safety, risk of identity theft, financial loss to an individual

Low risk data breach	A loss or exposure of aggregated data only, or of individual level data in circumstances where it is reasonably believed that no harm could occur (e.g. paper files are left behind in a meeting but quickly retrieved).
Medium risk data breach	A loss or exposure of personal information where it is reasonably believed that the third-party recipient does not have a malicious intent, and that the data is somewhat protected (e.g. laptop with encrypted data left on a bus).
High risk data breach	It is reasonably believed that the data breach is likely to result in serious harm to one or more of the individuals to whom the information relates (e.g. external hackers breach Council's firewall and copy valuable customer data).

Version history

Version	Approval date	Approved by	ECM reference	Change
1	5 December 2023	General Manager	S004-T00014	New Policy as required by Part 6A of the *Privacy and Personal Information Protection Act 1998 (NSW)* (PPIP Act) which establishes the NSW Mandatory Notification of Data Breach (MNDB) Scheme.

Internal use only

Responsible officer		Corporate Manager, Governance and Information		Approved by	General Manager
Minute		ECM reference	S004-T00014	Effective date	5 December 2023
Report		Review date	Minimum 18 Months	Pages	13