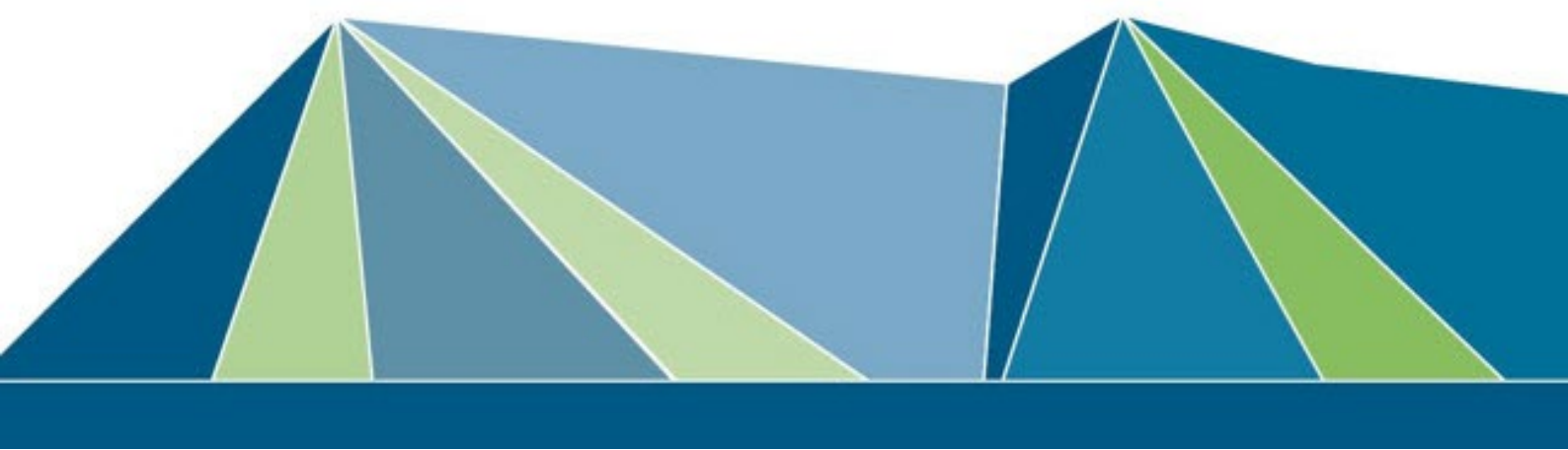
ballina shire council

Data Breach Response Plan

Version 1 November 2023



Data Breach Response Plan - External

Version	Date	Reason/Comments	Name/Position
1.0	November 2023		Stewart Littleford Manager Information Services

ballina
shire council

40 cherry street • po box 450 • ballina nsw 2478
t 1300 864 444 • **e** council@ballina.nsw.gov.au

ballina.nsw.gov.au

DATA BREACH RESPONSE PLAN - EXTERNAL

Table of Contents

OBJECTIVE

This plan sets out how Ballina Shire Council will manage a data breach, including the considerations around notifying persons whose privacy may be affected by the breach.

Effective breach management, including notification where warranted, assists Council in avoiding or reducing possible harm to both the affected individuals/organisations and the Council, and may prevent future breaches.

DEFINITIONS

Data breach means an incident in which there has been unauthorised access to, unauthorised disclosure of, or loss of, personal information held by Ballina Shire Council.

Personal information means information or an opinion about an individual whose identity is apparent or can reasonably be ascertained from the information or opinion.

This will include, but is not limited to, information about our staff, residents and ratepayers, suppliers and other contacts. It can include details such as name, address, phone number, email address, date of birth, tax file number or ratepayer records, licence details etc.

Individuals may still be identifiable even if steps have been taken to de-identify information (for example, removing direct identifiers or aggregating data). As such, it is prudent to treat de-identified information as personal information in the event of a data breach.

Notifiable data breach means a data breach which meets certain criteria, such as to trigger a legal requirement to notify the affected individuals, and/or appropriate regulator.

Low risk data breach means a loss or exposure of aggregated data only, or of individual level data in circumstances where it is reasonably believed that no real harm could occur (for example. paper files are left behind in a meeting but quickly retrieved).

Medium risk data breach means a loss or exposure of personal information where it is reasonably believed that the third-party recipient does not have malicious intent, and that the data is somewhat protected (for example, a laptop with encrypted data is left on a bus).

High risk data breach means 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 (for example, external hackers breach our firewall and copy valuable customer data). What we call a ‘high risk’ data breach will be a ‘notifiable’ data breach, unless it falls under one of the exceptions to the notification rules.

Serious harm includes such things as serious physical, psychological, emotional, financial, or reputational harm. Examples of harms could include identity theft, financial loss or blackmail, threats to personal safety, loss of business or employment opportunities, humiliation, stigma, embarrassment, damage to reputation or relationships, discrimination, bullying, marginalisation, or other forms of disadvantage or exclusion.

Likely to result in serious harm means the risk of serious harm to an individual is more probable than not. To help assess the likelihood that an individual might suffer serious harm if their personal information was lost, or subject to unauthorised access or unauthorised disclosure, there are a number of factors to consider. See the list of factors at Appendix A, in relation to assessing the likelihood of serious harm.

SCOPE OF PLAN

This plan applies to

- Council employees
- Councillors

RELATED DOCUMENTATION

Related documents, policies and legislation:

- Notifiable Data Breach Scheme - Privacy Act 1998
- Privacy Act 1988 (Cth)
- Privacy and Personal Information Protection Act 1998
- BSC Cyber Incident Response Plan

PLAN

What Is A Data Breach ?

A data breach occurs when there is a failure that has caused or has the potential to cause unauthorised access to Council data, such as;

- Accidental loss or theft of classified material data or equipment on which such data is stored (for example, loss of paper record, laptop, iPad or USB stick)
- Unauthorised use, access to, or modification of data or information systems (for example, sharing of user login details (deliberately or accidentally) to gain unauthorised access or make unauthorised changes to data or information systems)
- Unauthorised disclosure of classified material information (for example, email sent to an incorrect recipient or document posted to an incorrect address or addressee), or personal information posted onto the website without consent
- Compromised user account (for example, accidental disclosure of user login details through phishing)
- Failed or successful attempts to gain unauthorised access to Council information or information systems
- Equipment failure
- Malware infection
- Disruption to or denial of IT services

A data breach most commonly, but not exclusively, results in unauthorised access to, or the unauthorised collection, use, or disclosure of, personal information.

Responding to a Data Breach

Both the General Manager and Council's Privacy Officer must be informed of any data breach to ensure the application of this protocol and any subsequent advice to the Information Privacy Commissioner to assist in responding to enquiries made by the public, and managing any complaints that may be received as a result of the breach.

There are four key steps required in responding to a data breach;

1. Contain the breach and conduct a preliminary assessment.
2. Evaluate and mitigate the risks associated with the breach.
3. Notify and communicate.
4. Prevent further breaches.

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

1. Contain the breach and conduct a preliminary assessment

- Immediately take all realistic steps to contain the breach and limit any further access or distribution of the affected personal information
- Conduct preliminary fact-finding about the breach
- Make a preliminary assessment of the risk posed by the breach
- For high rated breaches, the Privacy Officer should activate the Breach Response Team immediately, to oversee the remainder of the breach response process.

2. Evaluate and mitigate the risks associated with the breach

- As soon as practicable, take remedial action to prevent or lessen the likelihood that the breach will result in harm to any individual.
- Complete an assessment of the harm that may eventuate from the breach.

  The assessment must determine whether there are reasonable grounds to believe that the data 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 assessment must be completed as soon as practicable, and at the very latest within 30 calendar days. Ideally, the assessment should be done within 2-3 days.
- To determine what other steps are needed, an assessment of the type of data involved in the breach and the risks associated with the breach will be undertaken.

  Some types of data are more likely to cause harm if it is compromised. For example, personal information, health information, and security classified information, will be more significant than names and email addresses on a newsletter subscription list.

  A combination of data will typically create a greater potential for harm than a single piece of data (for example, an address, date of birth and bank account details, if combined, could be used for identity theft).

Factors to consider include

- Who is affected by the breach?

  The assessment will include reviewing whether individuals and organisations have been affected by the breach, how many individuals and organisations have been affected and whether any of the individuals have personal circumstances which may put them at particular risk of harm.
- What was the cause of the breach?

  The assessment will include reviewing whether the breach occurred as part of a targeted attack or through inadvertent oversight.

  Was it a one-off incident or does it expose a more systemic vulnerability?

What steps have been taken to contain the breach?

Has the data been recovered?

Is the data encrypted or otherwise not readily accessible?

- What is the foreseeable harm to the affected individuals/organisations?

  The assessment will include reviewing what possible use there is for the data.

  For example, could it be used for identity theft, threats to physical safety, financial loss, or damage to reputation?

  Who is in receipt of the data?

  What is the risk of further access, use or disclosure, including via media or online?

3. Notify and Communicate

Council recognises that notification to individuals/organisations affected by a data breach can assist in mitigating any damage for those affected individuals/organisations and reflect positively on Council's reputation. Notification demonstrates a commitment to open and transparent governance, consistent with Council's approach.

However reflective of established guidance Council adopts the approach that if the data breach creates a real risk of serious harm to the individual, the affected individuals should be notified. The General Manager and Privacy Officer are to jointly make the determination as to the severity of the data breach.

In general, if a data breach creates a risk of harm to an individual/organisation, the affected individual/organisation should be notified. Prompt notification in these cases can help to avoid or lessen the damage by enabling the individual/organisation to take steps to protect themselves.

Notification is required by law under the PPIP Act if personal information and/or health information was involved and the assessment has concluded that there are reasonable grounds to believe that the data breach has resulted in, or is likely to result in serious harm to one or more of the individuals to whom the information relates (ie; what we describe as a High Risk breach).

Notification is required by law under the federal Privacy Act if TFNs were involved and the assessment has concluded that there are reasonable grounds to believe that the data breach has resulted in, or is likely to result in serious harm to one or more of the individuals to whom the information relates (ie; what we describe as a High Risk breach).

Notification is voluntary in all other cases (ie; Low Risk and other Medium Risk breaches). Consider the reasonable expectations of the individuals concerned, as well as our reputation as to whether we do or don't notify.

If we choose to voluntarily notify affected individuals, we do not need to notify the regulator, though it is best practice to do so nonetheless.

Mandatory notification requires the Privacy Officer, in conjunction with the General Manager and the Manager Communication and Customer Service to prepare a statement:

- In relation to a data breach involving personal and/or health information, the statement must be sent to the NSW Privacy Commissioner (part of the Information and Privacy Commission or IPC) immediately.

  The IPC can be contacted via email to ipcinfo@ipc.nsw.gov.au, or telephone on 1800 472 679.

- In relation to a data breach involving TFNs, the statement must be sent to the Australian Privacy Commissioner (Office of Australian Information Commissioner, OAIC) as soon as practicable.

- In relation to a data breach involving data received under the DSGS Act, the statement must be sent to the data provider and the NSW Privacy Commissioner (part of the Information and Privacy Commission or IPC) as soon as practicable.

  The IPC can be contacted via email to ipcinfo@ipc.nsw.gov.au, or telephone on 1800 472 679.

- The statement must also be provided directly to affected individuals as soon as practicable.

  See further information below about how to do this - refer to 'Appendix C - How to Notify Individuals'.

  NOTE - Where police or another law enforcement agency is investigating the breach, they must be consulted first, before making details of the breach public.

  There are limited exceptions to the requirement to notify individuals, such as if notification would prejudice an investigation or court proceedings, breach a secrecy provision, or create a serious risk of harm.

- If the data breach involves a contracted service provider, or other agencies, a joint notification should be made on behalf of all organisations, by the organisation with the closest relationship to the affected individuals.

There are occasions where notification can be counterproductive. For example, the information collected may be less sensitive and notifying individuals about a privacy breach which is unlikely to result in an adverse outcome for the individual may cause unnecessary anxiety and de-sensitise individuals to a significant privacy breach.

Factors Council will consider when deciding whether notification is appropriate include:

- What is the risk of harm to the individual/organisation?
- What steps has Council taken to date to avoid or remedy any actual or potential harm?
- What is the ability of the individual/organisation to take further steps to avoid or remedy harm?
- Even if the individual/organisation would not be able to take steps to rectify the situation, is the information that has been compromised sensitive, or likely to cause humiliation?

  The logistics of notifying affected individuals/organisations will depend in large part on the type and scale of the breach, as well as immediately practical issues such as having contact details for the affected individuals/organisations.

The Manager Communications and Customer Service will support the Breach Response Team by providing advice to customer facing teams about handling enquiries from customers. A set of FAQs are prepared to assist this process.

A proactive media/social media/communications response should also be developed with the support of the Manager Communications and Customer Service supporting the Breach Response Team. By publishing Ballina Shire Council's stated position early, we demonstrate our transparency and commitment to resolving this matter.

Affected individuals/organisations should be notified directly - by telephone, letter, email or in person. Indirect notification, such as information posted on Council's website, a public notice in a newspaper, or a media release, should generally only occur where the contact information of affected individuals/organisations are unknown, or where direct notification is prohibitively expensive or could cause further harm (for example, by alerting a person who stole the laptop as to the value of the information contained).

If there is a risk that the personal information could be used for identity theft or other types of fraud, we should engage with IDCARE, the National Identity & Cyber Support Service, on 1800 595 170, or via www.idcare.org. IDCARE can offer advice, and can also assist affected individuals.

There may be others we should contact, such as our insurance company, professional or other regulatory bodies, credit card companies, financial institutions, or credit reporting agencies, other internal or external parties, such as third-party contractors, or outsourcing agencies.

Also consider groups which represent the affected individuals, such as the relevant union if data about staff was compromised.

In some cases, we may need to consider offering compensation. Legal advice must be obtained before making any suggestions or offers to affected individuals.

What to Say

The notification advice will be tailored to the circumstances of the particular breach. The content of a notification could include:

- information about the breach, including when it happened
- a description of what data has been disclosed
- assurances (as appropriate) about what data has not been disclosed
- what the agency is doing to control or reduce the harm
- what steps the person/organisation can take to further protect themselves and what the BSC will do to assist people with this
- contact details for the BSC for questions or requests for information
- the right to lodge a privacy complaint with the Privacy Commissioner

4. Prevent Further Breaches

- For any high risk or medium risk breaches, the Privacy Officer must submit a report within 10 working days to the Breach Response Team and General Manager outlining the organisational response and mitigation plan. Regular updates may also be expected as matters unfold.
- High Risk breaches must be added to Ballina Shire Council's internal register of eligible (ie; notifiable/high risk) data breaches.
- Mitigation steps must address the identified root cause of the breach.

  Mitigation may include: a security audit and any modifications to physical controls such as locks, alarms, visitor access control, review of policies and procedures including the privacy management framework, review of employee training and selection practices, a review of suppliers and third parties, updating passwords, or altered deployments of technology.
- A review of the process used for this breach, after it has been handled, should be conducted, reported to the Breach Response Team and General Manager with details of any recommendations, and saved for future reference.
- Appropriate records must be maintained, to provide evidence of how suspected breaches are managed, including low, medium and high-risk breaches. Tracking data breaches allows Ballina Shire Council to monitor, analyse and review the type and severity of suspected and actual breaches.
- Conduct an annual review of our breach response records, to help identify and remedy: (i) weaknesses in security or processes that are prone to error, and (ii) any deficiencies in our response procedure which impact on its effectiveness.

REVIEW

This plan is to be reviewed every four years.

APPENDIX A - FACTORS TO CONSIDER IN ASSESSING SERIOUS HARM

The **assessment** about the **likelihood of serious harm** should have regard to:

- the type of information involved: for example, was it name and address, financial, health, criminal records, evidence of identity documents or other unique identifiers, biometrics, other types of 'sensitive information' such as information about a person's ethnicity, religion or sexuality? ('Sensitive information' is defined at s.19(1) of the PPIP Act.)
- the volume of information involved: was it a combination of pieces of data about the individual which would not otherwise be known?
- the number of individuals affected: for example, is there a risk that due to the number of people impacted, there is a higher chance that someone in the cohort may experience serious harm as a result of the breach?
- whether the information is protected by one or more security measures: for example, what is the likelihood that any of the security measures could be overcome?
- the risk profile of the information involved: for example, could it be used for identity theft or other fraudulent purposes? to humiliate or blackmail the individual? to commit physical harm?
- the type of individuals affected: for example, are the individuals experiencing vulnerability (for example, victims of family violence), or are the individuals involved worth targeting in some way (for example, very wealthy people or public figures)?
- how much time passed between becoming aware of the data breach and containing it?
- the context: was this an isolated incident, a systemic problem, a deliberate attempt to steal data, or the result of an accident or other unintentional behaviour?
- how likely is it, that the persons who may have obtained the information have an intention to cause harm to any of the individuals affected by the data breach?
- the further effects: is there a risk of ongoing breaches or further exposure of the information?
- the risk of cumulative harm: have there been breaches in other organisations that could result in a cumulative effect of more serious harm?
- the extent to which the risk has been successfully prevented or lessened by any remedial action or containment efforts: for example, was the data encrypted, was the portable storage device remotely wiped, were the hard copy files quickly recovered?
- given all of the above, the type of harm likely to affect the individuals: for example, identity theft, financial loss, threat to physical safety, threat to emotional wellbeing, loss of job opportunities, humiliation, damage to reputation or relationships, workplace or social bullying or marginalisation.

APPENDIX B - CONTENTS OF MANDATORY NOTIFICATION STATEMENT

The mandatory notification statement to impacted individuals must set out;

- the date the breach occurred.
- a description of the breach.
- how the breach occurred.
- the type of breach that occurred (i.e. unauthorised disclosure, unauthorised access, loss of information).
- the personal information that was the subject of the breach.
- the amount of time the personal information was disclosed for.
- actions that have been taken or are planned to ensure the personal information is secure, or to control or mitigate the harm done to the individual.
- recommendations about the steps the individual should take in response to the data breach (for example, link to www.idcare.org if the breach suggests we need to assist individuals protect against identity theft).
- information about making of privacy related complaints and internal reviews of certain conduct of public sector agencies.
- the name and contact details of the public sector agency the subject of the breach.
- if more than 1 public sector agency was the subject of the breach, the name of each other agency.

The mandatory notification statement to the IPC must use the approved form, and must set out:

- the information provided to impacted individuals (as set out above),
- a description of the personal information that was the subject of the breach,
- whether the head of the agency is reporting on behalf of other agencies involved in the same breach,
- if the head of the agency is reporting on behalf of other agencies involved in the same breach, the details of the other agencies,
- whether the breach is a cyber incident,
- if the breach is a cyber incident, details of the cyber incident,
- the estimated cost of the breach to the agency,
- the total number, or estimated total number, of individuals affected or likely to be affected by the breach, and notified of the breach,
- whether the individuals notified have been advised of the complaints and internal review procedures under the PPIP Act.

APPENDIX C – HOW TO NOTIFY INDIVIDUALS

There are three options for notifying individuals at risk of serious harm, depending on what is 'practicable':

1. Directly notify only those individuals at risk of serious harm, or
2. Directly notify all individuals whose data was breached, or
3. Publicise the statement more broadly.

ID Support NSW can assist us to identify and notify affected individuals.

Where it is possible to identify and contact only those individuals at risk of serious harm, Ballina Shire Council must directly notify those individuals. We might also publish the notification more broadly, including on our website.

Where it is not possible to identify which individuals might be at risk of serious harm, but it is possible for us to directly contact all individuals whose data was breached, then Ballina Shire Council will directly notify all individuals whose data was breached. We might also publish the notification more broadly, including on our website.

Where it is not reasonably practicable to identify which individuals might be at risk of serious harm, and it is not practicable to directly contact all individuals whose data was breached (for example, if we don't have up-to-date contact details for old customers), then we must publish a notification on our website, in a 'public notification register'.

We must also take reasonable steps to publicise that notification, for example we should consider other methods of communication such as social media, or advertisements in newspapers.

Where appropriate, social media will be used to provide information about the investigation, any updates and what further action individuals may take and what steps Ballina Shire Council is taking to prevent any future data breaches. A media response should also be considered.