Wentworth SHIRE COUNCIL

ANABRANCH
BURONGA
COOMEALLA
CURLWAA
DARETON
ELLERSLIE
GOL GOL
MONAK
POMONA
POONCARIE
RUFUS RIVER
TRENTHAM CLIFFS
WENTWORTH

Data Breach Policy

DOC/23/20246
Policy No: GOV027
Approved: 22 November 2023

If you require assistance reading and understanding this document, please contact the Translating and Interpreting Service on 131 450 and ask them to call Wentworth Shire Council on 03 5027 5027.

INTERPRETER SERVICES

IMPORTANT | ENGLISH

If you require assistance reading and understanding this document, customer service staff of Wentworth Shire Council are happy to assist in the arrangement of a free interpretive service.

To arrange an interpreter, please contact Council on 03 5027 5027, or visit a Council Office listed below.

MAHALAGA | FILIPINO

Kung kailangan mo ng tulong sa pagbabasa at pag-unawa sa dokumentong ito, ang mga kawani ng customer service ng Wentworth Shire Council ay masaya na tumulong sa pag-aayos ng isang libreng serbisyo ng interpretive. Upang ayusin ang isang interpreter, mangyaring makipag-ugnayan sa Council sa 03 5027 5027, o bisitahin ang isang Council Office na nakalista sa ibaba.

IMPORTANT | FRANÇAIS

Si vous avez besoin d'aide pour lire et comprendre ce document, le personnel du service client du Wentworth Shire Council se fera un plaisir de vous aider à organiser un service d'interprétation gratuit. Pour organiser un interprète, veuillez contacter le Conseil au 03 5027 5027 ou visitez un bureau du Conseil indiqué ci-dessous.

ΣΗΜΑΝΤΙΚΟ | ΕΛΛΗΝΙΚΟ

Εάν χρειάζεστε βοήθεια για την ανάγνωση και την κατανόηση αυτού του εγγράφου, το προσωπικό εξυπηρέτησης πελατών του Wentworth Shire Council είναι πρόθυμο να σας βοηθήσει στη διευθέτηση μιας δωρεάν υπηρεσίας διερμηνείας. Για να κανονίσετε έναν διερμηνέα, επικοινωνήστε με το Δήμο στο 03 5027 5027 ή επισκεφθείτε ένα Γραφείο του Συμβουλίου που αναφέρεται παρακάτω.

IMPORTANTE | ITALIANO

Se hai bisogno di assistenza per leggere e comprendere questo documento, il personale del servizio clienti del Wentworth Shire Council sarà lieto di assisterti nell'organizzazione di un servizio interpretativo gratuito. Per organizzare un interprete, contattare il Comune allo 03 5027 5027 o visitare uno degli uffici del Comune elencati di seguito.

PENTING | MELAYU

Jika anda memerlukan bantuan membaca dan memahami dokumen ini, kakitangan perkhidmatan pelanggan Wentworth Shire Council berbesar hati untuk membantu dalam pengaturan perkhidmatan tafsiran percuma. Untuk mengatur jurubahasa, sila hubungi Majlis di 03 5027 5027, atau lawati Pejabat Majlis yang disenaraikan di bawah.

重要 | 普通话(简体中文)

如果您在阅读和理解本文件时需要帮助，温特沃斯郡议会的客户服务人员很乐意协助安排免费口译服务。如需安排口译员，请致电 03 5027 5027 联系市议会，或前往下列市议会办公室。

ਮਹੱਤਵਪੂਰਨ | ਅੰਗਰੇਜ਼ੀ

ਜੇਕਰ ਤੁਹਾਨੂੰ ਇਸ ਦਸਤਾਵੇਜ਼ ਨੂੰ ਪੜ੍ਹਨ ਅਤੇ ਸਮਝਣ ਵਿੱਚ ਸਹਾਇਤਾ ਦੀ ਲੋੜ ਹੈ, ਤਾਂ ਵੈਨਟਵਰਥ ਸ਼ਾਇਰ ਕਾਉਂਸਲਿ ਦੇ ਗਾਹਕ ਸੇਵਾ ਸਟਾਫ ਇੱਕ ਮੁਫ਼ਤ ਵਿਆਖਿਆ ਸੇਵਾ ਦੇ ਪ੍ਰਬੰਧ ਵਿੱਚ ਸਹਾਇਤਾ ਕਰਨ ਲਈ ਖੁਸ਼ ਹਨ। ਦੁਭਾਸ਼ੀਏ ਦਾ ਇੰਤਜ਼ਾਮ ਕਰਨ ਲਈ, ਕਰਿਪਾ ਕਰਕੇ 03 5027 5027 'ਤੇ ਕਾਉਂਸਲਿ ਨਾਲ ਸੰਪਰਕ ਕਰੋ, ਜਾਂ ਹੇਠਾਂ ਸੂਚੀਬੱਧ ਕਸਿੇ ਕਾਉਂਸਲਿ ਦਫ਼ਤਰ 'ਤੇ ਜਾਓ।

สำคัญ | แบบไทย

หากคุณต้องการความช่วยเหลือในการอ่านและทำความเข้าใจเอกสารนี้ เจ้าหน้าที่บริการลูกค้าของ Wentworth Shire Council ยินดีให้ความช่วยเหลือในการจัดการบริการล่ามฟรี หากต้องการจัดเตรียมล่าม โปรดติดต่อสภาที่ 03 5027 5027 หรือไปที่สำนักงานสภาตามรายการด้านล่าง

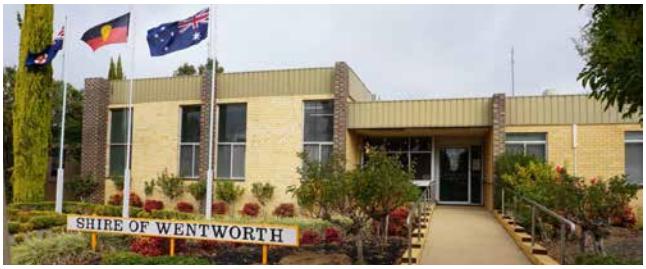
ÖNEMLİ | TÜRKÇE

Bu belgeyi okuma ve anlama konusunda yardıma ihtiyacınız varsa, Wentworth Shire Belediyesi'nin müşteri hizmetleri personeli, ücretsiz tercümanlık hizmetinin ayarlanmasında yardımcı olmaktan mutluluk duyacaktır. Bir tercüman ayarlamak için lütfen 03 5027 5027 numaralı telefondan Belediye ile iletişime geçin veya aşağıda listelenen bir Belediye Ofisini ziyaret edin.

QUAN TRỌNG | TIẾNG VIỆT

Nếu bạn cần trợ giúp để đọc và hiểu tài liệu này, nhân viên dịch vụ khách hàng của Hội đồng Wentworth Shire sẵn lòng hỗ trợ sắp xếp dịch vụ thông dịch miễn phí. Để sắp xếp một thông dịch viên, vui lòng liên hệ với Hội đồng theo số 03 5027 5027 hoặc đến Văn phòng Hội đồng được liệt kê bên dưới.

Midway Community Centre
6 Midway Drive, Buronga NSW 2739



Wentworth Shire Council Main Office
26-28 Adelaide Street, Wentworth NSW 2648

DATA BREACH POLICY

POLICY OBJECTIVE

The purpose of this policy is to provide guidance to Wentworth Shire Council employees on how to quickly and effectively respond to and manage a data breach and, in particular, an eligible data breach, to enable Council to comply with the NSW Mandatory Notification of Data Breach (MNDB) Scheme.

POLICY STATEMENT

This policy sets out how Council will respond to data breaches involving personal information. Council acknowledges that not all data breaches will be eligible data breaches but regardless Council takes all data breaches seriously. The policy details:

- what constitutes an eligible data breach under the PPIP Act
- roles and responsibilities for reporting, reviewing and managing data breaches
- the steps involved in responding to a data breach and reviewing systems, policies and procedures to prevent future data breaches.

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

POLICY COVERAGE

The scope of this policy applies to all data held by Council whether it is digital or hard copy and is applicable to all employees (including councillors, contractors and volunteers) as well as external contractors who have been granted access to Council's infrastructure, services and data.

1. STRATEGIC PLAN LINK

Objective: 4.0 Wentworth is supported by a strong and ethical civic leadership with all activities conducted in an open, transparent and inclusive manner.

Strategy: 4.2 Provide a strong, responsible and representative government.

2. DEFINITIONS AND ABBREVIATIONS

Term/Word	Definition
Council	Wentworth Shire Council
Council held information	For the purpose of this policy means any personal information in whatever form (whether hard copy or digital) which is held by Council or is otherwise in the possession or control of Council
Data Breach	A data breach occurs when personal or health information held by an agency is subject to unauthorised access, unauthorised disclosure or is lost in circumstances where the loss is likely to result in unauthorised access or unauthorised disclosure
Eligible Data Breach	Means a data breach as above AND where 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
MNDB Scheme	Means Mandatory Notification of Data Breach scheme established by Part 6A of the *Privacy and Personal Information*

DATA BREACH POLICY

	Protection Act 1998 (NSW) for mandatory reporting and notification of an eligible data breach
Personal Information	means any information defined as 'personal information' under the *Privacy and Personal Information Protection Act* 1998 (NSW). For the purpose of the MNDB Scheme 'personal information' includes 'health information', as defined in section 6 of the *Health Records and Information Privacy Act* 2002 – this means information about an individual's physical or mental health, disability, and information connected to the provision of a health service.

3. POLICY CONTENT

4.1 What is a data breach?

A data breach occurs when information held by Council is subject to unauthorised access, unauthorised disclosure, or is lost in circumstances where the loss is likely to result in unauthorised access or unauthorised disclosure.

A 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, unauthorised access, or theft of data or equipment on which data is stored (e.g. loss of paper records, laptop, iPad or USB stick);
- Unauthorised use, access to, or modification of data or information systems (e.g. sharing of user login details (deliberately or accidentally) to gain unauthorised access or make unauthorised changes to data or information systems);
- Unauthorised disclosure of personal information (e.g. email sent to an incorrect recipient or document posted to an incorrect address or addressee), or personal information posted onto the website without consent;
- A compromised user account (e.g. 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; and
- Disruption to or denial of IT services.

This policy discusses all data breaches and specifically provides for mandatory reporting of *eligible data breaches* under the PPIP Act.

The MNDB Scheme applies where an 'eligible data breach' has occurred. For a data breach to constitute an 'eligible data breach' under the MNDB Scheme, there are **two tests to be satisfied**:

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**

DATA BREACH POLICY

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.

The term 'serious harm' is not defined in the PPIP Act. Harms that can arise as the result of a data breach are context-specific and will vary based on:

- the type of personal information accessed, disclosed or lost, and whether a combination of types of personal information might lead to increased risk;
- the level of sensitivity of the personal information accessed, disclosed or lost;
- the amount of time the information was exposed or accessible, including the amount of time information was exposed prior to the agency discovering the breach;
- the circumstances of the individuals affected and their vulnerability or susceptibility to harm (that is, if any individuals are at heightened risk of harm or have decreased capacity to protect themselves from harm);
- the circumstances in which the breach occurred; and
- actions taken by the agency to reduce the risk of harm following the breach.

Serious harm occurs where the harm arising from the eligible data breach has, or may, result in a real and substantial detrimental effect to the individual. The effect on the individual must be more than mere irritation, annoyance or inconvenience.

Harm to an individual includes physical harm; economic, financial or material harm; emotional or psychological harm; reputational harm; and other forms of serious harm that a reasonable person in the agency's position would identify as a possible outcome of the data breach.

4.2 Systems and process for managing a data breach

Council has established a range of systems and processes for preventing and managing data breaches.

Council maintains an effective and integrated risk management framework, allocating resources, responsibility and accountability to manage risks across the organisation in accordance with AS ISO 31000:2018.

Council also has a range of supporting policies to control and mitigate exposure to breaches of data. This includes an *IT Incident Management Policy, Information Security Policy, Privacy Management Plan and Policy, Records Management Policy,* and *Code of Conduct.*

In addition to the policy controls, Council has a comprehensive set of IT controls, including robust access controls, network and endpoint security measures, data loss prevention systems, and incident response plans. An up-to-date inventory of assets is maintained, along with strong pathway and vulnerability management measures, to ensure all IT assets are properly secured and monitored. Regular training is provided to employees and penetration tests are performed to identify and remediate weaknesses in the IT infrastructure.

Council will require all contracts with contractors who may be provided with, have access to, or hold Council held information, to contain obligations requiring the contractor to report a data breach to their Contract Manager at Council and to take mitigating actions and assist Council in undertaking assessments of a data breach. Contracts will also identify who will notify any affected individuals and provide support in the event of a data breach.

4.3 Reporting and Responding to a data breach

The sooner Council can detect a data breach the better the chance that it may be contained, potential harms mitigated through prompt action, and assessment commenced to identify whether

DATA BREACH POLICY

the breach may be an eligible data breach with appropriate actions taken.

Council may be made aware of a data breach through a report from an employee, a contractor, an affected individual, or through a report from another government agency.

Council also undertakes various monitoring activities and utilises monitoring services and cyber security networks as tools that provide for early identification of a data breach of Council held information.

The Director Corporate Services must be informed of any data breach to ensure the application of this policy, including making notifications to the Privacy Commissioner for eligible data breaches and affected individuals.

There are five key steps required in responding to a data breach:

1. Initial report and triage

2. Contain the breach

3. Assess and mitigate

4. Notify

5. Review.

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

The Director Corporate Services will coordinate with the Manager Technology Services and/or service providers to address and respond to identified data breaches related to its IT systems.

Step One: Initial Report and Triage

A staff member, contractor or third-party provider is to notify the Director Corporate Services within one business day of becoming aware that a data breach has occurred and provide information about the type of data breach as detailed in Section 4.1 of this Policy. The Director Corporate Services will notify the General Manager immediately of a suspected eligible data breach and will review the information provided to determine whether it is an eligible data breach under the MNDB Scheme. A data breach report and action plan will be prepared and details recorded in an Internal Data Breach Register and held in Council's Record Management System. Members of the public are also encouraged to report any data breaches to Council in writing by using the contact options available on Council's website. The General Manager may consider convening a Data Breach Response Team where a data breach involves highly sensitive information, has a high risk of harm to individuals and affects more than one individual.

Step Two: Contain the Breach

Containing the breach is prioritised by Council. All necessary steps possible 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 led to the breach, or 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 legal or other advice on what action can be taken to recover the data. When recovering data, Council will make sure that copies have not been made by a third party or, if they have, that all copies are recovered.

Step Three: Assess and Mitigate

DATA BREACH POLICY

To determine what other steps are needed, Council will undertake an assessment of the type of data involved in the breach, whether the breach is an eligible breach under the MNDB Scheme, and the risks and potential for serious harm associated with the breach. The data breach report and action plan will be used for reporting on the investigation of the breach and authorising actions in response – this is to be provided to the General Manager for approval.

The Director Corporate Services will be responsible for the implementation of proposed actions and recommendations.

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?** Council's 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?** Council's assessment will include reviewing whether the breach occurred as part of a targeted attack or through inadvertent oversight. Questions include: Was it a one-off incident, has it occurred previously, or does it expose a more systemic vulnerability? What steps have been taken to contain the breach? Has the data or personal information been recovered? Is the data or personal information encrypted or otherwise not readily accessible?

• **What is the foreseeable harm to the affected individuals/organisations?** Council's assessment will include reviewing what possible use there is for the data or personal information. This involves considering the type of data in issue (including personal information subject to special restrictions under s.19(1) of the PPIP Act), if it could it be used for identity theft, or lead to 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? If case-related, does it risk embarrassment or harm to a client and/or damage Council's reputation?

Upon becoming aware of a possible data breach Council will take into account the Statutory Guidelines issued by the IPC including Guidelines on the assessment of data breaches under Part 6A of the PPIP Act.

In order to mitigate the breach, Council will consider implementation of additional security measures within Council's own systems and processes to limit the potential for misuse of compromised information.

Step Four: Notify

If an eligible data breach has occurred, the notification process under Division 3 of the MNDB Scheme (Part 6A of the PPIP Act) is triggered. There are four elements of the notification process:

1. Notify the Privacy Commissioner immediately after an eligible data breach is identified using the approved form.

2. Council will address Statutory Guidelines issued by the IPC to determine whether an exemption applies: If one of the six exemptions set out in Division 4 of the MNDB Scheme applies in relation to an eligible data breach, Council may not be required to notify affected individuals.

3. Notify individuals: Unless an exemption applies, notify affected individuals or their authorised representative as soon as reasonably practicable.

DATA BREACH POLICY

4. Provide further information to the Privacy Commissioner.

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, consistent with Council's strategic plan. If a data breach is not an eligible data breach under the MNDB Scheme, Council may still consider notifying individuals/organisations of the breach dependent upon the type of information that is involved, the risk of harm, repeated and/or systematic issues and the ability of the individual to take further steps to avoid or remedy harm.

Notification should be undertaken promptly to help to avoid or lessen the damage by enabling the individual/organisation to take steps to protect themselves. The MNDB Scheme requires an agency to take reasonable steps to notify affected individuals as soon as practicable.

The method 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. Considerations include the following:

When to notify

Individuals/organisations affected by a data breach will be notified as soon as practicable. Whilst this policy sets a target of notification within 5 days; practical factors are also recognised. Where all individuals affected by an eligible data breach cannot be notified, Council will consider issuing a public notification on its website.

How to notify and what to say

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 is unknown, or where direct notification is prohibitively expensive or could cause further harm (for example, by alerting a person who stole the laptop as to the value of the information contained). A record of any public notification of a data breach will be published on Council's website and recorded on a Public Data Breach Register which will be developed for this purpose for a period of twelve months.

Council's notification will address the considerations set out under sections 59O and 59P of the PPIP Act.

Other obligations including external engagement or reporting

For every data breach Council will consider other internal and external notifications and arrangements and communicate with such external agencies and stakeholders as is reasonably required in the individual circumstances of a particular data breach. This could include NSW Police; the Australian Federal Police; Cyber Security NSW; the Australian Cyber Security Centre where a data breach involves malicious activity from a person or organisation outside Australia; the Office of the Australian Information Commissioner (OAIC) if the breach involves Tax File Numbers; and financial service providers where required.

Step Five: Review

Council will further investigate the circumstances of the breach to determine all relevant causes and consider what short or long-term measures could be taken to prevent any reoccurrence. Council will undertake recommended steps to further mitigate and remediate Council's procedures, policies and IT systems to prevent future data breaches.

A post breach review and evaluation may include a:

DATA BREACH POLICY

- review of Council's IT systems and remedial actions to prevent future data breaches;
- security audit of both physical and technical security controls;
- review of Council's risk management and privacy management policies and procedures;
- review of employee training practices;
- review of contractual obligations with contracted service providers.

Any recommendations to implement the above preventative actions are to be approved by the General Manager and documented in Council's record management system.

Reporting of relevant matters will be provided to Council's Audit Risk and Improvement Committee and to Council.

4.4 Roles and Responsibilities

The following staff have identified roles under this policy:

- Councillors as the governing body are responsible for periodic review and endorsement of this policy;
- The Director Corporate Services is responsible for implementing this policy, reporting data breaches to the General Manager and all notifications and actions for eligible data breaches;
- The Director Corporate Services is responsible for investigating data breaches, preparing a data breach report and action plan and developing and maintaining internal and public registers for data breaches;
- The Manager Technology Services is responsible for ensuring that appropriate and auditable IT incident management procedures are in place and applied during/review of any incident;
- All Council employees, contractors and consultants have a responsibility for immediately reporting a suspected data breach in accordance with this policy to their Manager or Director.

4. RELATED DOCUMENTS & LEGISLATION

Legislation

Privacy and Personal Information Protection Act 1998 (NSW)

Government Information (Public Access) Act 2009 (NSW)

Privacy Act 1988 (Cwth)

Policies

GOV007 - Council's Privacy Policy

GOV013 – Council's Risk Management Policy

GOV020 – Council's Code of Conduct

GOV022 – Council's Compliance Policy

OP/GOV201 – Records & Information Management Policy

OP/GOV223 - Council's Operational IT Incident Management Policy

OP/WF539 - Council's Operational Information Security Policy

Council's Privacy Management Plan

DATA BREACH POLICY

5. ATTACHMENTS

Nil.

6. DOCUMENT APPROVAL

This document is the latest version of the official policy of the Wentworth Shire Council, as adopted by Council on 15 November 2023.

This policy may be amended or revoked by Council at any time.

A PDF copy of the signed document can be accessed from Council's record management system and Reliansys.

Signed: .....

22 Nov 2023

General Manager Wentworth Shire Council **Date**

Version	Date	Author	Changes
0.1	6/11/2023	D. Zorzi	-
1.0	15/11/2023	D. Zorzi	Adopted by Council 15 November 2023 with minor amendments – First Release

This page intentionally left blank

Wentworth SHIRE COUNCIL

Contact

Main Service Centre
26-28 Adelaide Street, Wentworth

Postal Address
PO Box 81, Wentworth NSW 2648

(03) 5027 5027

council@wentworth.nsw.gov.au

wentworth.nsw.gov.au

Have Your Say:
wentworth.nsw.gov.au/have-your-say