DISTRICT COUNCIL OF Streaky Bay

Policy Document

PERSONAL INFORMATION SECURITY POLICY

Policy No: **DCSB-IFM-13.05**	Version No: **1.1**	Administered by: **Chief Executive Officer**
Approved by: **Council**	Approved on: **15 October 2020**	Agenda Item/Minute Book No or Approval Ref: **316/20**
Last Reviewed: **21 June 2018**	Review Date **October 2024**	File No: **F16/675**
Classification: **Information Management**		
Strategic Plan link: **Strategy 1.3** Ensure Council fulfils its legislated governance responsibilities and its decision-making is supported by relevant policies and codes.		

References and related Policies & Procedures:

Government of South Australia Information Privacy Principles Instruction
Privacy Amendment (Notifiable Data Breaches) Act 2017
Notifiable Data Breach Scheme: Guidelines for Councils
Government of South Australia Personal Information Data Breaches Guideline – Public I1-A1
Government of South Australia Information Security Management Framework
DCSB-IM-PROC-13.02 Notifiable Data Breach Procedure
DCSB-G-09.12 – Elected Members Records Management Policy
DCSB-IFM-13.06 Digitisation and Disposal Temporary Source Records Policy

Table of Contents

1. Introduction

The Commonwealth Privacy Act does not generally apply to South Australian Government agencies. However, an amendment to the Privacy Act, which came into effect in February 2018, requires all government agencies that hold tax file number (TFN) information to comply with the Commonwealth's Notifiable Data Breach Scheme, but only in respect to TFN breaches.

2. Purpose

This Policy has been developed to provide advice regarding the identification and notification of inappropriate disclosure of personal information held by the District Council of Streaky Bay. Such disclosure will be termed a "Personal Information Data Breach" within this Policy.

3. Objectives

The objectives of this policy are to:

- promote positive relations between the Council and its community;
- ensure the security of personal information stored by Council;
- comply fully with legislative requirements with regards to reporting under the Notifiable Data Breach Scheme; and
- ensure Council staff understand their roles fully in the event of a data breach.

4. Principles

This policy is underpinned by the following principles, which are central to effective personal information data management. The Council will:

- ensure personal information is managed and maintained securely;
- recognise any potential data breach and report where the breach is notifiable;
- advise those people affected by any data breach as per the policy; and
- seek further advice regarding data breaches should it be required.

5. Policy

5.1 What is Personal Information?

5.1.1 In delivering Council services to the community, Council collects and manages large amounts of information and data, including personal information, on behalf of ratepayers and other trusted partners.

5.1.2 Personal information is information or an opinion, whether true or not, relating to a natural person, or the affairs of a natural person, whose identity is apparent, or can reasonably be ascertained. A natural person in this context is a living human being as per the *Information Privacy Principles Instruction (February 2017)*.

5.1.3 Personal information may include but is not limited to, combinations of name, address, date of birth, financial or health details, ethnicity, gender, or religion for example.

5.1.4 The personal information held by Council may be collected in paper form, verbally or through electronic means.

5.1.5 Where it has been identified there has been a Personal Information Data Breach, Council will take prompt action to deal with the breach and inform appropriate parties.

5.2 How is personal information collected, managed and used by Council?

5.2.1 The collection, management and use of personal information is governed by the South Australian *Information Privacy Principles Instruction – Premier and Cabinet Circular PC012* (PC012). The South Australian *Data Sharing Act 2016* provides boundaries around specific uses of the personal information collected and held by Council.

5.2.2 The *Commonwealth Privacy Act* (the Privacy Act) does not generally apply to South Australian Government agencies, including local Councils.

5.2.3 An amendment to the Privacy Act, came into effect in February 2018, which requires Council to comply with the Commonwealth's Notifiable Data Breaches Scheme as Council holds tax file number (TFN) information.

5.2.4 Refer to Attachment 3 of this Guideline for further information relating to data breaches involving TFN information.

5.3 What is a Personal Information Data Breach and how does in occur?

5.3.1 A Personal Information Data Breach occurs when official information that is not already publicly available, is lost or subjected to unauthorised access, use modification, disclosure or misuse.

5.3.2 Personal Information Data Breaches may occur in a number of ways, including accidental loss, internal errors or deliberate actions of trusted employees, theft of physical assets or the theft or misuse of electronic information (e.g. cyber-attack).

5.4 How will Council manage Personal Information Data Breaches?

5.4.1 When a Personal Information Data Breach is evident, Council will take prompt action to report the breach, identify the risks, notify relevant affected parties and implement remedial action.

5.4.2 Should a Personal Information Data Breach be identified, Security Policy and relevant procedures such as the Notifiable Data Breach Procedure will apply.

5.5 Who would be notified in the event of a Personal Information Data Breach?

5.5.1 Should a data breach occur that contains personal information, the Privacy Committee of South Australia will be notified.

5.5.2 The Chief Executive Officer (CEO) is responsible for the decision as to whether to notify parties affected by a data breach.

5.5.3 In general, if a data breach creates a real risk of serious harm to an individual or organisation, the affected parties will be notified.

5.5.4 Notification may not always be appropriate. Providing notification about low risk breaches may cause undue anxiety and de-sensitise individuals to notice.

5.5.5 Any incidence will be assessed on a case-by-case basis, to determine whether notification is required.

5.5.6 Appended to this Policy are tools to assist with identification of notification requirements when Personal Information Data Breach has occurred:

Attachment 1: Data Breach Notification Process

Attachment 2: Risk Assessment and Notification Tool.

5.6 Where may I access further advice?

5.6.1 Attachment 3 to this Policy is a listing of organisations Council may notify of a breach, or where Council or the community may seek further advice with regard to the management of Personal Information Data Breaches.

6. Alteration or Substitution of Policy

Any alteration or substitution of this policy with a new policy will require public consultation, unless the Council determines the alteration or substitution is only a minor signification and would attract little or not community interest.

7. Records

7.1 Recording of all information relating to any data breach will be maintained and kept by relevant departmental staff.

7.2 All records must be kept in accordance with Council's Records Management Guidelines, including the Elected Members Records Management Policy, and destroyed as per the current General Disposal Schedule.

8. Further Information

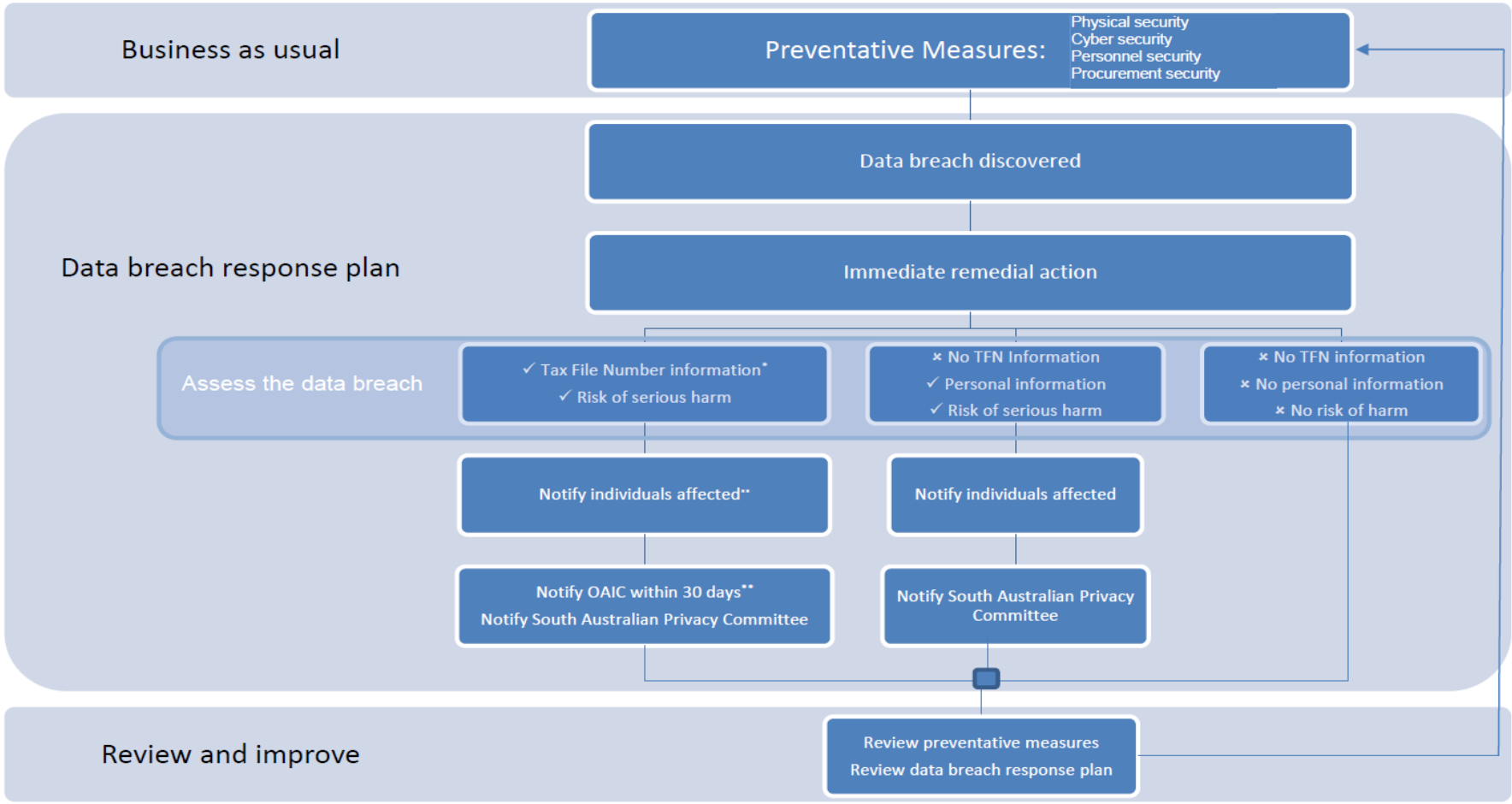
8.1 This policy will be available at Council's main office as listed below during ordinary business hours and available to be downloaded, free of charge, from Council's website at www.streakybay.sa.gov.au.

District Council of Streaky Bay – Main Office
29 Alfred Terrace
Streaky Bay SA 5680

9. Document History

Version	Change Description	Date	Author
1.0	New Document	21/06/2018	Karina Ewer
1.1	Update of document – revision due	15/10/2020	Karina Ewer

Attachment 1: Data Breach Notification Process



* Tax File Number information is information that connects a Tax File Number with the identity of an individual.

** The *Privacy Amendment (Notifiable Data Breaches) Act 2017* requires that that notifications to individuals affected and the notification to the Office of the Australian Information Commissioner (OAIC) both contain specific information. See www.oaic.gov.au for more information.

Government of South Australian (Public I2-A1)

Attachment 2: Risk Assessment and Notification

Assessing the Risk of Personal Data Breach

Once it is ascertained that a Personal Data Breach is likely to have occurred, the Manager, Business and Administrative Services (MBAS) will assess the risks associated with the data breach and whether affected parties should be notified.

The following factors will be considered as part of the risk assessment:

The type of information involved	Does the type of compromised information create a risk of harm? • Is it personal, commercial, medical, legal, security classified or other sensitive information? • Does the aggregate of information create greater risk or harm? Who is affected by the incident? Are those affected at particular risk? Has tax file number (TFN) information been disclosed?
The context of the information and the incident	What is the context of the information involved? How sensitive is it? What parties have gained unauthorised access to the affected information? Have there been other incidents that could have a cumulative effect? How could the information be used?
The cause and extent of the incident	Is there a risk of ongoing incidents or further exposure of the information? Is there evidence of theft? Was the information targeted? What was the source of the incident? Was it intentional or malicious? Is the information adequately encrypted, anonymised or otherwise not easily accessible? Has the information been recovered? What steps have already been taken to mitigate the harm? Is this a systemic problem or an isolated incident? How many individuals or organisations are affected by the incident?

The risk of harm to those affected	Who is the recipient of the information? What harm to individuals or organisations could result from the breach? Examples of harm include: • identity theft; • financial loss; • threat to physical safety or emotional wellbeing; • loss of business or employment opportunities; • damage to reputation or relationships; • bullying or marginalisation; and / or • insider trading or unfair commercial advantage
The risk of other harms	Are there any other possible harms that could occur, including to the Council as a result of the incident?

In general, if a data breach creates a real risk of serious harm to an individual or organisation, the affected parties should be notified.

Notification of Personal Data Breaches may however, not always be appropriate. Providing notification regarding low risk breaches may cause undue anxiety and de-sensitise individuals to notice. Each incident needs to be assessed on a case-by-case basis to determine whether notification is required.

Prompt notification to those affected in these cases can help them mitigate the damage by taking steps to protect themselves. The MBAS will:

- take into account the ability of the individual or organisation to take specific steps to mitigate such harm;
- consider if there are any legal, regulatory or contractual obligations to notify; and
- consider whether it is appropriate to inform third parties such as the police, or other regulators or professional bodies about the data breach incident.

Notifying affected parties

At the point that notification is being considered, the Chief Executive Officer (CEO) will have as complete a set of facts as possible and will complete a risk assessment based on the facts gathered. Sometimes the urgency or seriousness of the incident may dictate that notification should happen immediately, prior to all facts being gathered and assessments having been undertaken.

When to notify	Those affected will be notified as soon as possible. If it is a criminal matter, checks will be completed with law enforcement authorities prior to notification so as not to compromise any ongoing investigations.
How to notify	Affected parties will be notified directly – by phone, letter, email, or in person. Indirect notification (e.g. on a website) will only be appropriate where direct notification has provide impossible, unfeasible, or may cause further harm.
Who should notify	The Manager, Corporate Services, or the CEO will notify those affected. This includes where a breach may have involved handling of information by a third party service provider or contractor.
Who should be notified	Generally, the individuals(s) or organisation affected by the incident will be notified. In some cases it may be appropriate to notify an individual's guardian or authorised representative on their behalf. The Information Privacy Principles Instruction will be considered should this be required. If the breach contains TFN information then the OAIC will need to be notified under the Notifiable Data Breaches Scheme, including specific requirements which apply for notifying individuals affected.

What should be included in the notification	The information in the notification should help those affected to reduce or prevent harm that could be caused by the incident. Information may include: • a description of the incident; • the type of information disclosed; • what has been done to respond to the incident and reduce harm; • assistance available to those affected and steps they can take to reduce harm; • sources of information that could assist those affected; • contact information for the Council where those affected may need more information to address concerns; • whether the incident has been notified to a regulator or other external party; and / or • how individuals may lodge a complaint. The wording of the notification may have legal implications, and secrecy obligations may also apply. The Council may consider seeking legal advice prior to notification as a result. If notification is required under the Australian Data Breaches Notification Scheme, specific requirements apply and will be adhered to.
Who else should be notified	Provide details of the data breach and response to Council's CEO. Notifying authorities or regulators will not be a substitute for notification of those affected. In some circumstances it will be appropriate or necessary to notify the following parties: • State Records; • The Privacy Committee of South Australia; • South Australian Government Chief Information Security Officer; • Insurers or others due to contractual obligations; • Credit card companies or financial institutions; • Regulatory bodies may have notification requirements;

	• Agencies that have a direct relationship with the information exposed (e.g. Medicare in the case of Medicare numbers); and / or • Office of the Australian Information Commissioner.

Important Considerations

Notifying parties affected by a data breach is considered good practice. The Council has responsibility to promote open and transparent government, assist in building public trust in government and enable individuals and organisations to exercise control over their information, privacy and security.

- The Government of South Australia Information Privacy Principles Instruction regulates the way in which personal information can be collected, used, stored and disclosed by Councils. Personal information is defined as information or an opinion, whether true or not, relating to a natural person or the affairs of a natural person whose identity is apparent, or can reasonably be ascertained, from the information or opinion.

The decision on how to notify will be made on a case-by-case basis. In some cases, Council may choose to take additional actions that are specific to the nature of the incident.

- As part of the initial assessment of a security incident, the Manager, Corporate Services will be immediately informed.
- Law enforcement, internal investigation, across government response organisations and other regulatory bodies may be notified as required by relevant policy or legislation.
- Where law enforcement authorities are investigating the incident, the CEO will consult with the investigating agency prior to making details of the incident public.

Attachment 3: Contact Organisations for Advice

Below is a list of organisations Council may be required to notify, or may consider notifying, if a data breach occurs.

Privacy Committee of South Australia

- Data breaches involving personal information held by Council should be reported to the Privacy Committee.
- The Executive Office of the Committee can also provide general advice on the Information Privacy Principles Instruction and obligations of reporting.
- State Records and the Privacy Committee can be contacted on:
    - **Phone** (Business Hours): (08) 8204 8791
    - **E-mail** (Business Hours) staterecords@sa.gov.au
    - **Website**: www.archives.sa.gov.au/

Department of Premier and Cabinet, Office for Cyber Security

- All data breaches that involve information stored or communicated electronically must be reported to the Office for Cyber Security as a cyber security incident. Information on how to lodge a report can be found at https://digital.sa.gov.au/resources/topic/policies-guidelines-and-standard/security/information-security-management-framework
- The Office for Cyber Security may also be able to provide advice and assistance on the ICT aspects of managing the data breach and preventative measures.
- Report cyber security incidents to the Office for Cyber Security as the Control Agency for Cyber Crisis on:
    - **Phone** (Business Hours): (08) 8226 7513
    - **E-mail** (Business Hours) WatchDesk@sa.gov.au
    - **Duty Officer** (Emergency/Out of Hours number): (08) 8232 3049

South Australia Police

- If the data breach may be a result of criminal actions, the Police will be notified as soon as practicable.
- Notification of those affected by the data breach will be delayed until advice from the Police is received, as notification may compromise a criminal investigation.
- The Police may be contacted on the number below, or visit your local police station: **Phone** (24 hours) 131 4444

Office of the Australian Information Commissioner

- If the data breach relates to tax file number (information), and it is likely it will result in serious harm to individuals, the Office of the Australian Information Commissioner (OAIC) must be advised in accordance with the Australian Government's Notifiable Data Breaches scheme (The Scheme)
- The Scheme specifies the information that must be included in the notifications for those affected, the timeframe for notification i.e. as soon as practicable within 30 days of the breach being discovered, and the requirement to notify the Australian Information Commissioner of the breach.
- Information regarding how to report a breach to the OAIC as per the Information Security Policy.

Additional Contacts

The following will need to be considered depending on the data that was compromised:

- **Any other organisation that is the source of the information that was compromised**. For example, if Tax File Numbers or Medicare Numbers were contained in the compromised information, then the Australian Taxation Office or Medicare respectively should also be notified of the breach.
- **Insurers** relevant to the breach such as professional or public liability insurers for the Council or any Cyber Risk Insurance held with regard to particular data sets.
- **Financial institutions or credit card companies**. They may be able to assist in notifying individuals or reducing the impact of those affected.
- **Other internal or external parties**. Consider if any other third parties may have been affected by the breach. For example, if information about a particular government tender process was breach, all organisations that submitted a tender, even if their information wasn't included in the breach, may need to be notified. Some parties to consider include:
    - Other internal business unites not already notified that may have a need to know (e.g. communications, human resources, senior management group).
    - Other government departments that may experience some impact from the breach.
    - Unions or other employee representatives, particularly if any employee information was compromised.
- **Regulatory bodies:**
    - **Australian Securities and Investment Commission**. Companies and registered corporations have reporting requirements to ASIC.
    - **Australian Competition and Consumer Commission**. The ACCC has a role in protecting the interests and safety of consumers and as such they have their own data breach notification requirements. Also consider if individuals affected may contact the ACCC to make a complaint regarding the data breach.

- **Australian Communications and Media Authority**. ACMA have their own data breach reporting requirements if the data compromised includes Integrated Public Number Database (IPND) information.
- **Other regulatory bodies**. Council may need to consider contacting agencies such as the Local Government Authority, water licensing regulatory bodies or boards, education, infrastructure, health, justice and child protection sectors in particular depending on the compromised information. Each body will have differing notification requirements in case of a data breach.