Procedure Document

NOTIFIABLE DATA BREACH PROCEDURE

Procedure No: **DCSB-IM-PROC-13.02**	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: **317/20**
Last Reviewed: **New Procedure**	Review Date **October 2024**	File No: **F16/1192**
Classification: **Governance**		
Strategic Plan link: **Strategy 1.1.7** Ensure compliance of relevant Council policies and procedures with legislative requirements.		
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-IFM-13.06 Personal Information Security Policy DCSB-G-09.12 – Elected Members Records Management Policy DCSB-IFM-13.06 Digitisation and Disposal Temporary Source Records Policy		

Table of Contents

1. Purpose

1.1. This procedure has been developed to give instruction as to the steps required in the event of a Notifiable Data Breach.

1.2. A Notifiable Data Breach occurs when the Tax File Number (TFN) information held by Council is lost or subjected to unauthorised access, modification, disclosure, or other misuse or interference.

1.3. This procedure should be read in conjunction with the Security Policy and Personal Information Security Policy.

2. Definition of a Notifiable Data Breach

2.1. Notifiable Data Breaches occur when the TFN data of an individual or individuals is breached. Examples of a Notifiable Data Breach may include but are not limited to:

- loss or theft of laptops or USBs, or paper records that contain TFN information;
- unauthorised access to TFN information by an employee;
- inadvertent disclosure of TFN information due to 'human error', for example an email sent to the wrong person;
- hacking of a database containing TFN information.

2.2. In the event any Council employee becomes aware of a possible data breach they MUST notify the Manager, Corporate Services immediately.

2.3. Council have notification obligations for which the Manager, Corporate Services and the Chief Executive Officer (CEO) as responsible.

3. Responding to Data Breaches

3.1. Where a data breach has been identified the following steps must be undertaken:

3.2 Step 1: Contain

3.2.1 Once an employee discovers or suspects a data breach, they MUST immediately notify the Manager, Corporate Services.

3.2.2 The employee must provide as much information as possible to the Manager, Corporate Services as to the nature and extent of the possible data breach.

3.2.3 The Manager, Corporate Services must endeavour to immediately stop the unauthorised access, recover lost or stolen records, or change database access privileges to stop hacking (being careful not to destroy evidence that may be valuable in identifying the cause of the breach).

3.2.4 The Manager, Corporate Services must then consult with the CEO as to whether an eligible data breach has occurred.

3.3 Step 2: Assess

3.3.1 An eligible data breach only occurs when the following three criteria have been met:

- There is unauthorised access to, or unauthorised disclosure of, TFN information or a loss of TFN information held by Council.
- The access, disclosure or loss is *likely to result in serious harm* to one or more individuals.

  The term "likely to result" means the risk of serious harm to an individual is more probable than not (rather than possible).

  "Serious harm" can by psychological, emotional, physical, reputational, or other forms of harm. An assessment of serious harm will need to be made on a case by case basis.

- Council has not been able to prevent likely risk of serious harm by taking remedial action.

3.3.2 If it is not clear that a data breach meets all three criteria, the Manager, Corporate Services and the CEO MUST conduct an assessment to determine whether there is an eligible data breach that triggers notification obligations.

3.3.3 An assessment shall be conducted within 30 days, beginning from when the Manager, Corporate Services becomes aware of the data breach. An assessment must be reasonable and expeditious.

3.3.4 An assessment will contain and record the following three stages:

- Stage 1: Initiate:
  The CEO will decide whether an investigation is necessary and identify which person or group will be responsible for completing the investigation (Stage 2).

  The Manager, Corporate Services will be responsible for oversight of each investigation unless there is a real or perceived Conflict of Interest (see Conflict of Interest Policy).

  In the case of a Conflict of Interest the CEO will appoint an alternative Manager to undertake or oversee the investigation.

- Stage 2: Investigate:
  The appointed investigator or team will gather all relevant available information regarding the suspected data breach.

  Information will include but will not be limited to:
  - what information was compromised;
  - how the information was compromised (see 2.1 above);
  - what the nature of the compromise or intent was (for example, was the data breach deliberate, malicious, or accidental);
  - who may have had access to the information;
  - how many individuals may have been affected; and
  - what level of harm may be caused by the breach.

  A report MUST be made in writing by the lead investigator (Manager, Corporate Services, or where appointed another Manager) to the CEO once the investigation is finalised.

- Stage 3: Evaluate:
  The CEO must make a decision, based on the report from the lead investigator as to whether the incident is an eligible data breach (i.e. where TFN information has been compromised).

  Where the breach is found NOT to be an eligible data breach, internal remedial action will be required to ensure further incidents to not occur. Please see Step 3 below.

  Where the breach IS found to be an eligible data breach both Steps 3 and 4 will need to be undertaken in order to comply with legislative requirements.

3.4 Step 3: Take Remedial Action

General

3.4.1 Where remedial action is possible which will prevent the likelihood of serious harm occurring then the breach is NOT considered an eligible data breach and no notification is required.

3.4.2 Remedial action is adequate where it prevents the unauthorised access or disclosure of TFN information. An example of remedial action is where TFN information is sent to the wrong recipient via email. The recipient is contacted before they access the information and they confirm the data has not been copied and has been permanently deleted from their data files. Confirmation MUST be received in writing (including email) on such occasions.

3.4.3 A record regarding the successful remedial action must be saved to TRIM.

3.4.4 Remedial action should be taken as soon as possible, ideally during Step 1: Contain.

Non-eligible Data Breach

3.4.5 Where the information compromise has been remediated at Step 1, employees must still notify the Manager, Corporate Services.

3.4.6 The Manager, Corporate Services will notify the CEO as to the nature of the data compromise and how the incident has been remediated to this point.

3.4.7 A full understanding of the compromise occurrence will be investigated by the Manager, Corporate Services and recommendations as to business improvement practices will be sent to the CEO for consideration.

3.4.8 Business improvement practices may include but are not limited to such mitigation strategies as: changing individual data base access; changes to the ways in which data is received, handled or processed; and / or changes to the ways in which data is reported.

3.4.9 Where the CEO finds the business improvement practices to be adequate, these will be implemented in order to ensure further breaches of the same type do not occur in the future.

3.4.10 Notification of individuals may not be required in these instances.

3.4.11 Notification of individuals shall be at the discretion of the CEO as per the Personal Information Security Policy.

3.4.12 Should the notification of individuals be deemed necessary please refer to Attachment 1 as to how this will occur.

3.4.13 Notification to government reporting bodies are not required in instances where TFN information has not been compromised.

Eligible Data Breach

3.4.14 If remedial action is not taken, or is unsuccessful in preventing the likelihood of serious harm occurring, the CEO MUST notify of the eligible data breach.

3.5 Step 4: Notify

3.5.1 Where TFN information has been compromised, there is an eligible data breach the CEO must notify:

a. the Australian Information Commissioner via an online statement form, available at https://forms.business.gov.au/smartforms/landing.htm?formCode=OAIC-NDB. What to include in an eligible data breach statement may be referenced at Attachment 2; and

b. affected individuals as per Attachment 1.

3.5.2 Individuals must be notified of the data breach as soon as practicable after completing the statement for the Australian Information Commissioner.

3.5.3 Considerations of the cost, time and effort of notification may be relevant when deciding when to notify individuals however it is important notification occur as expeditiously and cost effectively as is possible.

3.5.4 Where individuals have been notified of a data breach prior to the Australian Information Commissioner being notified (as per 3.2 Step 1: Contain), they do not need to be notified again so long as the contents of the statement sent to the Commissioner were included in that notification.

3.6 Step 5: Review

3.6.1 Whether or not a data breach meets the threshold of an eligible data breach, the incident, including any relevant policies and procedures, must be reviewed.

3.6.2 Review will be conducted by the Manager, Corporate Services and must be completed within 30 days of the incident being finalised.

3.6.3 Review will address how the incident occurred and consider ways policies, procedures and current practices might be altered to ensure a similar incident does not occur in the future.

4. References, Links and Additional Information

- Notifiable Data Breach Scheme: Guidelines for Councils

5. Records

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

5.2 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.

6. Further Information

6.1. 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

7. Document History

Version	Change Description	Date	Author
1.0	New Document	July 2018	Karina Ewer
1.1	Update of document – revision due	15 October 2020	Karina Ewer

Attachment 1 – Notification of Individuals

Notification of individuals regarding data breaches will be determined depending on whether the data breach is deemed eligible (TFN information has been compromised) or ineligible for notification.

Eligible Data Breach (TFN Compromise) – Notification of Individuals

1. Where serious harm due to TFN compromise cannot be mitigated through remedial action, the CEO must ensure the notification of individuals at risk of serious harm and provide a statement to the Australian Information Commissioner as soon as practicable.

2. If it is not practicable to notify individuals, Council must publish a copy of the statement prepared for the Australian Information Commissioner on the District Council of Streaky Bay website, and take all reasonable steps to bring its contents to the attention of individuals at risk of serious harm.

3. If a single eligible data breach applies to multiple Councils, only one Council needs to notify the Commissioner and individuals at risk of serious harm. It is up to the Councils with the most direct relationship with the individuals at risk of serious harm to undertake the notification process.

4. There are three options the CEO is to consider as to how individuals may be notified of the data breach. Each option is outlined below.

5. Whether a particular option is practicable involves consideration of the time, effort, and cost of notifying individuals at risk of serious harm in a particular manner. Each factor should be considered in light of the capabilities and capacity of Council staff.

Option 1 – Notify all Individuals

6. If practicable, the CEO may request the Manager, Corporate Services to arrange for the notification of each individual to whom the relevant information relates. That is, all individuals whose personal information was part of the eligible data breach.

7. This option may be the most appropriate, and simplest method, if the investigator or investigation team cannot reasonably assess which particular individuals are at risk of serious harm from the eligible data breach. This may particularly be true where a data breach involves multiple individuals and it is therefore difficult to determine which one or more of those individuals is likely to face serious harm due to the data breach.

8. The benefit of choosing this option includes ensuring all individuals who may be at risk of serious harm are notified, and allowing them to consider whether they need to take any action in response to the eligible data breach.

Option 2 – Notify only those Individuals at Risk of Serious Harm

9. The CEO may choose to notify only those individuals who are at risk of serious harm from the eligible data breach.

10. If the investigation is able to identify only particular individuals, or a specific subset of individuals, involved in an eligible data breach as being at risk of serious harm, and those individuals are able to be specifically identified, then only those individuals need to be notified.

11. The benefit of this targeted approach is that Council may avoid causing unnecessary distress to those who are not at risk, which in turn limits the possibility of notification fatigue among members of the public, and reduces administrative costs.

    Example: An attacker installs malicious software on Council's website. The software allows the attacker to intercept payment card details when customers pay invoices through the Council website. The attacker is also able to access basic account details for all customers who have an account set up through the Council's website. Following a comprehensive risk assessment, the Council considers individuals who paid invoices during the period the malicious software was active are at likely risk of serious harm, due to the likelihood of payment card fraud. Based on this assessment, the Council also considers those customers who only had basic account details linked to the Council website are not at likely risk of serious harm as the information was not sufficient to gain access to accounts without further permissions. Council will only be required to notify those individuals it considers to be at likely risk of serious harm.

Option 3 – Publish Notification

12. Where the breach is an eligible data breach, and if neither option 1 or 2 above are practicable, for example, if the Council does not have up-to-date contact details for all individuals, then Council must:
    - publish a copy of the statement on its website; and
    - take reasonable steps to publicise the content of the statement.

13. It is not enough under the regulations to upload a copy of the statement prepared for the Australian Information Commissioner. The CEO and Manager, Corporate Services must take all proactive steps to publicise the substance of the eligible data breach (and

at least the contents of the statement), to increase the likelihood that the eligible data breach will come to the attention of the individuals at risk of serious harm.

14. The statement must remain accessible on Council websites and other relevant forums for at least 6 months.

Non-Eligible Data Breach (no TFN Compromise) – Notification of Individuals

15. Where a data breach does not involve TFN Information, the CEO will still consider which of the above options is most practicable in each situation.

16. The CEO may also decide not to notify individuals where the data breach does not involve TFN information and no individuals are deemed to be at serious risk of harm

17. Where a data breach is deemed not eligible for notification, a statement does not need to be prepared for the Australian Information Commissioner, so will not be included in the information sent to individuals.

Contents of Individual Notifications

18. Any method or combination of methods may be utilised to notify individuals concerning both eligible and non-eligible data breaches.

19. Methods of notification may include but are not limited to:
    - telephone calls;
    - SMS;
    - physical mail;
    - social media posts;
    - in-personal conversations

    as long as the method is reasonable.

20. When considering if a particular method or combination of methods is reasonable, the CEO should consider the likelihood the people being notified will become aware of, and understand the notification, and weigh this against the resources involved in undertaking notification.

21. All verbal forms of notification must have written notes made after the conversations and those notes saved into TRIM along with all other files relating to the particular incident.

22. All written files must be saved directly into TRIM along with all other files relating to the particular incident.

23. Council may notify an individual using their usual method of communicating with that particular individual. For example, if an entity usually communicates through an intermediary, Council may also choose to notify through this intermediary.

24. Council may also tailor the form of notification to individuals, as long as it includes the content outlined below.

25. Notification of individuals MUST include:
    - the Statement prepared for the Australian Information Commissioner (FOR ELIGIBLE DATA BREACHES ONLY);
    - the identity and contact details the individual may use to contact Council for more information regarding the data breach (generally this will be the Manager, Corporate Services);
    - a description of the data breach Council has reasonable grounds to believe has happened;
    - the kind(s) of information concerned;
    - information regarding any other authority notified of the breach (as per the Personal Information Security Policy) where that has been necessary; and
    - recommendations about the steps the individual might take in response to the data breach.

26. Decisions regarding the appropriate types of recommendations will always be dependent on the circumstances of the data breach. Recommendations may include choosing to tailor steps around an individual's personal circumstances, or providing general recommendations that apply to all individuals. In some instances, Council may have already taken some protective steps, reducing the necessity for action by affected individuals. Council may choose to explain these measures in the notification as part of the recommendations provided.

27. Where the data breach is an eligible data breach and direct contact of individuals is not possible, the CEO may decide to publish a copy of the statement prepared for the Commissioner on the District Council of Streaky Bay website.

    27.1. The purpose of publicising the statement in this instance is to draw it to the attention of individuals at risk of serious harm. The CEO would therefore

consider what mechanisms would be most likely to bring the statement to the attention of these people. Reasonable methods therefore might include:

- ensuring the notice is prominently placed on the relevant webpage, and easily located and accessed by the individuals concerned;
- publication of an announcement on Council's social media sites directing individuals to the website;
- taking out print or online advertising directing individuals to the website; and / or
- use of the Community Noticeboard to alert individuals to the website and statement

27.2. In some cases it might be reasonable to utilise more than one of the above options in order to publicise the data breach effectively. Where a data breach is of a broader nature, it might be necessary to consider multiple channels of communication in order to reach all affected individuals.

27.3. The CEO will consider the ability and likelihood of individuals at risk of serious harm being able to access the information when determining the appropriateness of relying solely on any one approach to notification.

28. Where the data breach is not eligible for reporting to the Australian Information Commissioner, the CEO may still decide to publish a statement on the District Council Streaky Bay website. That notification will have the information required at clause 24 included.

29. Should publication prove the only option for notification, the CEO and Manager, Corporate Services, will take care to ensure any online notice does not contain any personal information. For example it may be more appropriate to list the date range within which the data breach occurred to assist at risk individuals in self-identification. The notice will include contact details where those individuals may access further information.

Attachment 2: What to Include in an Eligible Data Breach Statement

A statement about an eligible data breach to the Australian Information Commissioner must include:

- the identity and contact details of the Council;
- a description of the eligible data breach;
- the kind or kinds of information involved in the eligible data breach; and
- what steps the entity recommends individuals take in response to the eligible data breach.

It must be remembered the only form of eligible data breach for Council to currently consider are those which include individual's TFN information.

Identity and contact details of the Council

The Statement must include the Council's full identity being the District Council of Streaky Bay. The contact details of at least the CEO and Manager, Corporate Services should also be included. The Council needs to include information regarding who individuals may contact in order to address and answer queries from affected individuals.

Description of the eligible data breach

A description of the data breach is to be included in the statement to the Australian Information Commissioner.

The statement must include sufficient information about the data breach to allow affected individuals the opportunity to properly assess the possible consequences of the data breach for them, and take protective action in response.

Information may include:

- the date, or a date range, of the unauthorised access or disclosure;
- the date the entity detected the data breach
- the circumstances of the data breach (such as any known causes for the unauthorised access or disclosure)
- who has obtained or is likely to have obtained access to the information
- relevant information about the steps the Council has taken to contain or remediate the breach.

Usually it will suffice to provide a general description of the type of person who has obtained the information such as 'an external third party' or 'a former employee'.

The Kind or Kinds of Information Concerned

In the case of an eligible data breach only TFN information is relevant for reporting purposes.

Steps recommended to individuals in response to the eligible data breach

The statement must include recommendations individuals should take in response to the data breach in order to mitigate the serious harm or likelihood of serious harm from the data breach.

The nature of the recommendations will depend on which Council functions or activities caused the eligible breach, the circumstances of the eligible data breach and the extent to which the TFN information was compromised. Recommendations should include practical steps that are easy for the individuals to action. In the case of TFN breaches recommendations may include contact with the Australian Taxation Office.

Additional Information to provide

Other Councils involved in the data breach

If more than one Council holds TFN information that was compromised in the eligible data breach, only one Council needs to prepare a statement and notify individuals about the data breach. Instances where this may occur are when the District Council of Streaky Bay has outsourced the handling of personal information, is involved in a joint venture, or where it has a shared services arrangement with another Council.

When a data breach affects more than one Council, the Council that prepares the statement may include the identity and contact details of the other Councils involved. Whether a Council includes the identity and contact details of other involved Councils in its statement will depend on the circumstances of the eligible data breach, and the relationship between the Councils and the individuals involved.