# Data Breach Response Plan

St Joseph's Primary School, Red Cliffs (SJPS) is committed to managing personal information in accordance with the Privacy Act 1988 (Cth) (the Act) and the SJPS Privacy Policy.

This document sets out the processes to be followed by staff in the event that SJPS experiences a data breach or suspects that a data breach has occurred. A data breach involves the loss of, unauthorised access to, or unauthorised disclosure of, personal information.

The *Privacy Amendment (Notifiable Data Breaches) Act 2017* (NDB Act) established a Notifiable Data Breaches (NDB) scheme requiring organisations covered by the Act to notify any individuals likely to be at risk of serious harm by a data breach. The Office of the Australian Information Commissioner (OAIC) must also be notified.

Accordingly, SJPS needs to be prepared to act quickly in the event of a data breach (or suspected breach), and determine whether it is likely to result in serious harm and whether it constitutes an NDB.

Adherence to this Procedure and Response Plan will ensure that SJPS can contain, assess and respond to data breaches expeditiously and mitigate potential harm to the person(s) affected.

This Procedure and Response Plan has been informed by:

- The Office of the Australian Information Commissioner's "Guide to developing a data breach response plan"
- The Office of the Australian Information Commissioner's "Data breach notification guide: a guide to handling personal information security breaches"
- NDB Act
- The Act and Australian Privacy Principles (Schedule 1 of the Act)

This document should be read in conjunction with SJPS Privacy Policy.

**Definition**
**Data Breach**
A data breach occurs when personal information is lost or subjected to unauthorised access, modification, use or disclosure or other misuse. Data breaches can be caused or exacerbated by a variety of factors, affect different types of personal information and give rise to a range of actual or potential harms to individuals, agencies and organisations.

**Notifiable Data Breach**
Where a data breach has occurred that is likely to result in serious harm to any of the individual to whom the information relates, it is considered *'eligible'* and must be reported to the Office of the Australian Information Commissioner (OAIC).

**Serious Harm**
'Serious harm' is not defined in the Privacy Act. In the context of a data breach, serious harm to an individual may include serious physical, psychological, emotional, financial, or reputational harm.

**Implementation**
This response plan is intended to enable SJPS to contain, assess and respond to data breaches in a timely fashion, to help mitigate potential harm to affected individuals. It clarifies the roles and responsibilities of staff, and the processes to assist the school to respond to a data breach (refer to Appendix A: Flow Chart: Data Breach Response Plan).

Some data breaches may be comparatively minor, and able to be dealt with easily without reporting to the OAIC. For example:

> *A staff member, as a result of human error, sends an email containing personal information to the wrong recipient. Depending on the sensitivity of the contents of the email, if the email can be recalled, or if the staff member can contact the recipient and the recipient agrees to delete the email, it may be that the issue is reported to the principal but does not require any further response.*

This should be documented including:

- Description of breach or suspected breach
- Action taken by the principal to address the breach or suspected breach
- The outcome of the action
- The principal's view that no further action is required

The principal will use their discretion in determining whether a data breach or suspected data breach requires an escalation of the data breach process. In making that determination, principal will consider the following questions:

- Are multiple individuals affected by the breach or suspected breach?
- Is there (or may there be) a real risk of serious harm to the affected individual(s)?
- Does the breach or suspected breach indicate a systemic problem in school processes or procedures?
- Could there be media or stakeholder attention as a result of the breach or suspected breach?

If the answer to any of these questions is 'yes', then it may be appropriate for the principal to notify the OAIC (refer to Risk Assessment Process).

*OAIC Advice Data Breach: What must be included* will assist the principal in notifying the OAIC.
https://www.oaic.gov.au/resources/agencies-and-organisations/guides/data-breach-notification-guide-august-2014.pdf

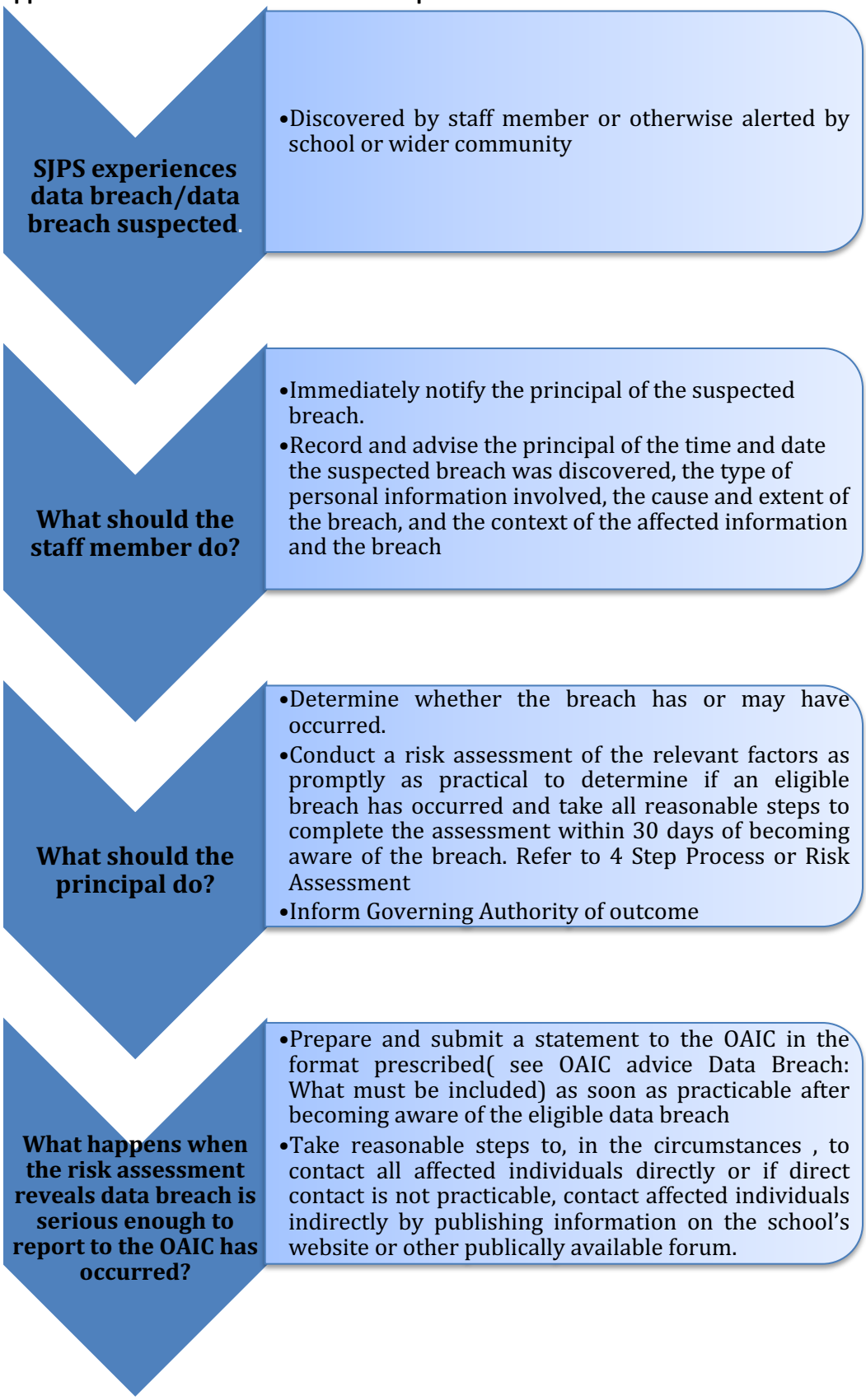
**Record Management**

Documents on breaches will be saved in a central file on school administration system.

Refer to:

- Appendix A: Flow Chart: Data Breach Response Plan
- Appendix B: Risk Assessment Process
- Appendix C: Data Breach Prevention Checklist (CECV)
- Appendix D: Individual Notification Record (CECV)
- Appendix E: Example of an Email to Parents/Carers (CECV)
- Appendix F: Data Breach Notification for Other Entities (CECV)
- Appendix G: Breach and Assessment Checklist (CECV)

**Appendix A: Flow Chart: Data Breach Response Plan**



**Appendix B: Risk Assessment Process**

**Process**

There is no single method of responding to a data breach. Data breaches must be dealt with on a case-by-case basis, by undertaking an assessment of the risks involved, and using that risk assessment to decide the appropriate course of action.

There are four key steps to consider when responding to a breach or suspected breach. The principal should ideally undertake steps 1, 2 and 3 either simultaneously or in quick succession.

**Step 1: Contain the breach and do a preliminary assessment**

- Convene a meeting with relevant staff and/or Leadership Team
- Ensure that all evidence of breach is preserved so that an assessment of the breach can be made

**STEP 2: Evaluate the Risks Associated with the Breach**

- Conduct an initial investigation, and collect information about the breach promptly including;
    - The date, time, duration and location of the breach
    - The type of personal information involved in the breach
    - How the breach was discovered and by whom
    - The cause and extent of the breach
    - A list of affected individuals, or possible affected individuals
    - The risk of serious harm to the affected individuals
    - The risk of other harms

- Determine whether the content of the information is important
- Establish the cause and effect of the breach
- Assess priorities and risks based on what is known
- Keep appropriate records of the suspected breach and actions of the response team, including the stapes taken to rectify the situation and the decisions made

**STEP 3: Notification**

- Determine who needs to be made aware of the breach (internally and potentially externally) at this preliminary stage
- Determine whether to notify affected individuals is there a real risk of serious harm to the affected individuals? In some cases, it may be appropriate to notify the affected individuals immediately; e.g., where there is a high level of risk of serious harm to affected individuals
- Consider whether others should be notified, including police/law enforcement, or other agencies or organisations affected by the breach, or where the school is contractually required or required under the terms of an MOU or similar obligation to notify specific parties

**STEP 4: Prevent Future Breaches**

- Fully investigate the cause of the breach
- Report to Governing Authority on outcomes and recommendations:
    - Update security and response plan if necessary.
    - Make appropriate changes to policies and procedures if necessary
    - Revise staff training practices if necessary
    - Consider the option of an audit to ensure necessary outcomes are affected

## Appendix C: Data Breach Prevention Checklist (CECV)

| Item to be checked | Setup correct | Comments |
|---|---|---|
| **PHYSICAL CHECKS** | | |
| Servers and computers, and storage devices storing data which have the potential to harm individuals or the school are stored in a locked and alarmed area after hours. | | |
| Access to these areas are restricted to authorized personnel by means of separate key types and security codes. | | |
| All areas are checked that they are securely shut at the end of each day. | | |
| Alarmed areas are checked when alarms are activated. | | |
| Stolen computers to be reported to police. | | |
| Paper records are shredded or disposed of by placing in a locked bin and properly disposed of by a professional company hired for the purpose. | | |
| Security contractors check the campus daily. | | |
| **COMPUTER SECURITY** | | |
| All computers require password login. | | |
| Staff passwords are required to be changed regularly according to a set security procedure. | | |
| Access to various data is governed by login credentials. | | |
| Bulk transfer of data on removable media is to be avoided but may be approved by management and removed from media after transfer | | |
| Bulk download of data is to be avoided but may be approved by management if required. Data is deleted from computers after specific use. | | |
| Bulk communication (email, SMS) do not allow users to see others' data (Use of Bcc in emails) | | |
| Erasing of all data on laptops before they are permanently removed from the school (staff and students leaving; laptops donated to others) | | |
| **NETWORK SECURITY** | | |
| Administration access by restricted personnel. | | |
| Firewall rules set to prevent unauthorized access. | | |
| Student and staff networks are separated. | | |
| Intranet access is restricted by network login credentials or parental login credentials. | | |
| **COMMUNICATIONS SECURITY** | | |
| Student email is web-based and filtered for unauthorized access and malware. | | |
| Staff email is server-based and filtered for unauthorized access and malware. | | |
| **PERSONNEL SECURITY** | | |
| Visitors need to sign a register when arriving and leaving the campus. | | |
| Locks to servers or areas containing classified information are different to the general locks to areas accessible for general staff. | | |
| Keys are allocated to staff according to security clearance level. | | |
| Contractors are supervised on campus. | | |
| **POLICIES and PROCEDURES** | | |
| Privacy Policy available on school website for anyone to review | | |
| Staff, students, parents and affected others are made aware of the school's privacy policy. | | |
| Procedures available to govern the collection, input, access, retention and disposal of data | | |
| Approval of all service delivery partners' privacy policies | | |
| **TRAINING** | | |
| Staff training on correct procedures involving the collection, input, access, retention and disposal of data | | |

**Appendix D: Individual Notification Record (CECV)**

**Date of breach**: **Time of breach**:

**Date and time breach was reported**:

**Data Breach Description**:

**Assessed level of risk**:

**Individual directly affected**:

*There may be circumstances where parents, carers or authorised representatives should be notified as well as, or instead of, the individual.*

**Individual Notification**

| Person notified | Person sending notification | Contact details of person notified | Notification Date | Acknowledgement date |
|---|---|---|---|---|
| | | | | |

**Notification Details:**

*A copy of email or written description sent to the individual should be placed below and should include the following headings:*

- **Incident Description** and **Type of personal information involved**

- **Response to the breach**

- **Assistance offered to affected individuals**

- **School contact details**

- **How individuals can lodge a complaint with the school**

**Appendix E: Example of an email to Parents/Carers (CECV)**

*Dear Mr and Mrs Smith*

*We are writing to inform you of an incident that has the possibility of exposing your contact information to unauthorised people or organisations.*

*On June 8, 2107, a CEM staff members USB memory stick with a file containing your names, your home address, email addresses and phone numbers (home and mobile) was reported missing. While we are attempting to locate the USB stick, we believe it would be prudent to consider any actions you need to take to mitigate and possible harm.*

*In particular, please take note of any unsolicited calls or emails. Should such events occur, please consider changing your details and please inform the school of such occurrences and inform us of your new contact details.*

*We sincerely apologise for the inconvenience or harm this may cause. We are reviewing our procedures regarding the storage of sensitive information on portable media such as USB memory sticks and will implement any procedural changes required in an attempt to avoid such events in future.*

*Please do not hesitate to contact me if you wish to discuss the matter further.*

*Yours sincerely*

*Principal*

*School*

## Appendix F: Data Breach Notification for Other Entities (CECV)

**Form:**

This form should be used when preparing to inform other entities that may be impacted by the data breach.

**Complete each section**

1. **A description of the breach**
2. **The type of personal information involved**
3. **How many people were or may have been affected**
4. **When the breach occurred**
5. **When and how the school became aware of the breach**
6. **The cause of the breach**
7. **Whether the breach was inadvertent or intentional**
8. **Whether the breach appears to stem from a systemic issue or an isolated trigger**
9. **Whether the breach has been contained**
10. **What action has been taken or is being taken to mitigate the effect of the breach and/or prevent further breaches**
11. **Any other entities involved**
12. **Whether the school has experienced a similar breach in the past**
13. **Any measures that were already in place to prevent the breach**
14. **Whether a data breach response plan was in place, and if it has been activated**
15. **The name and contact details of an appropriate person within your organisation**
16. **Any other relevant factors.**

**Appendix G: Breach and Assessment Checklist (CECV)**

**Checklist**

**Date of breach**: **Time of breach**:

**Date and time breach was reported**:

**Data Breach Description**:

| Action | Person/s Responsible | Comment |
|---|---|---|
| **CONTAIN THE BREACH** | | |
| Stop the unauthorised practice | | |
| Recover the records | | |
| If possible or if it would not compromise evidence, shut down the system that was breached | | |
| If it is not practical to shut down the system, or if it would result in loss of evidence, then revoke or change computer access privileges | | |
| Address weaknesses in physical or electronic security | | |
| **PRELIMINARY ASSESSMENT** | | |
| Appoint someone to lead the initial assessment | | |
| Is there is a need to assemble a team | | |
| What personal information does the breach involve? | | |
| What was the cause of the breach? | | |
| What is the extent of the breach? | | |
| What are the harms (to affected individuals) that could potentially be caused by the breach? | | |
| How can the breach be contained? | | |
| **EARLY NOTIFICATION** | | |
| Who needs to be made aware of the breach (internally, and potentially externally)? | | |
| List affected individuals | | |
| Escalate to management as appropriate – person for privacy compliance | | |
| Do police need to be informed? | | |
| Is serious harm to individuals possible? | | |
| Is high level media attention likely? | | |
| Complete “Notification Record” (Step 3) | | |
| **OTHER MATTERS** | | |
| If laws have been broken, consult before going public with details | | |
| Be careful not to destroy evidence | | |
| Keep records of the suspected breach and the steps taken to rectify the situation and the decisions that are made. | | |