Catholic Schools Office
Diocese of Lismore

DATA BREACH
STANDARD OPERATING PROCEDURE

SOP Number:	DBSOP01:03
Status:	Ratified
Date Issued:	February 2018
Evaluation and Review:	February 2020
SOP Contact Officer:	Assistant Director - School Resources Services
Related Documentation:	Catholic Education in the Diocese of Lismore Foundational Values for Catholic Identity and Mission
	Digital and Social Media Policy
	Employee Performance and Discipline Policy and Standard Operating Procedure
	Privacy Policy and Standard Operating Procedure
	Education Act 1990 (NSW)
	Privacy Act 1988 (Cth)

RATIONALE

The Catholic Schools Office (CSO) and all parish schools create, collect and maintain a vast amount of data, much of which is confidential personal information of students and employees. The data collected is used in relation to mandatory record keeping requirements.

Information retained by the CSO and parish schools is held in many forms such as student and employee records, reports, personnel records, health records, paper files, and computerised databases and documents. It may be transmitted in many ways including by hand, by courier, or electronically using shared communications lines. Information may be transmitted through systems controlled by the CSO or parish schools or systems controlled by external parties. The principles underlying the need for information security applies to all information irrespective of the platform on which it is held.

Recent changes to the Commonwealth *Privacy Act 1988* make it compulsory for the CSO and parish schools that experience a data breach to have procedures in place to contain, access, respond and notify those affected or the Commissioner when necessary in a timely manner.

A data breach is an incident, in which personal or confidential information, or non-personal information that could be sensitive or commercial, is compromised, disclosed, copied, transmitted, accessed, removed, destroyed, stolen or used by unauthorised individuals, whether accidentally or intentionally.

This Standard Operating Procedure outlines the procedural obligations on all employees to identify, report, and address a data breach.

SCOPE

This Standard Operating Procedure applies to all employees in parish schools, the Catholic Schools Office and any related entities under the administration of the Catholic Schools Office, Diocese of Lismore.

1. DEFINITIONS

1.1 **Commissioner** means the Office of the Australian Information Commissioner.

1.2 **Confidential Information** means information that is controlled and only available on a need to know basis in order for employees to perform their duties.

1.3 **Data Breach** means an incident in which personal or confidential information, or non-personal information that could be sensitive or commercial, is compromised, disclosed, copied, transmitted, accessed, removed, destroyed, stolen or used by unauthorised individuals, whether accidentally or intentionally.

1.4 **Data Breach Response Team** means the team of personnel from the CSO who will provide advice and/or manage all data breaches in parish schools or the CSO. Members of the Data Breach Response Team will be advised to CSO and parish school staff. See section 2 – Data Breach Response Team.

1.5 **Data Collection** means the systematic gathering of data for a particular purpose from various sources, including entries made into software systems, questionnaires, interviews, application forms, existing records and electronic devices.

1.6 **Notifiable Data Breach** means the following:

I. When there is unauthorised access to, unauthorised disclosure of, or loss of, personal information held by the CSO or a parish school; and

II. The access, disclosure or loss is likely to result in serious harm to any of the individuals to whom the information relates.

1.7 **OAIC** means the Office of the Australian Information Commissioner.

1.8 **Personal Data** means information or an opinion whether true or not, about an individual, and whether recorded in a material form or not, about an individual whose identity is apparent, or can reasonably be ascertained from the information or opinion.

1.9 **Personal Health Information** means all health information where the identity of a person is apparent or can be reasonably ascertained from the information itself. Information is also personal information if it is reasonably possible for the person receiving the information to identify the individual by using other information that they already hold.

1.10 **Public Information** means information that is approved as suitable for public dissemination by legislation or routine disclosure.

1.11 **Risk Assessment** means the identification, evaluation and estimation of the levels of risk involved in a situation.

1.12 **Serious Harm** means serious physical, psychological, emotional, economic and financial harm, as well as serious harm to reputation and other forms of serious harm that a reasonable person would identify as a possible outcome of the data breach.

2. DATA BREACH RESPONSE TEAM

2.1 The CSO will have in place a Data Breach Response Team to manage data breaches that affect the CSO or parish schools.

2.2 The Data Breach Response Team shall comprise of the CSO ICT Manager and the CSO eLearning and Data Consultant. The Data Breach Response Team may consult the CSO Risk Committee where necessary.

2.3 All suspected and actual data breaches at a parish school or CSO level are managed by the Data Breach Response Team. Management includes the provision of advice and referral back to the parish school to manage where appropriate.

2.4 The process of communication with the Data Breach Response Team is as follows:

I. Contact the CSO or a Data Breach Response Team member if a direct contact number is known;

II. The breach is then to be logged onto the CSO ICT Helpdesk. This provides a method of record keeping;

III. The Data Breach Response Team will perform a preliminary assessment of the breach;

IV. If appropriate, the management of the breach will be referred back to the parish school to manage data breaches of a less serious nature, following the processes outlined in this Standard Operating Procedure, or for remedial action (See section 4 – Remedial Action).

3. NOTIFIABLE DATA BREACH

3.1 If a CSO or a parish school employee has reasonable grounds to believe that a data breach has occurred, the CSO Data Breach Response Team must be notified in the first instance.

3.2 If a notifiable data breach has occurred in the circumstances defined in 1.6, the Data Breach Response Team must notify the Commissioner and the affected individuals of the breach on behalf of the CSO if a CSO breach, or on behalf of a parish school if a parish school breach.

3.1 Examples of a data breach include the following:

I. Hacking of the school's system through malicious software;

II. Disgruntled employees taking data with them when they leave the school;

III. By innocent error, such as sending personal information by email to the wrong email address; and

IV. A portable device containing personal information being lost or stolen.

3.2 Each of these scenarios may give rise to an obligation on the CSO or parish school to comply with the requirements of the Notifiable Data Breach scheme.

3.3 In deciding whether a reasonable person would conclude that a data breach would be likely to result in serious harm to an individual, the following factors may be relevant:

I. The kind of information;

II. The sensitivity of the information;

III. The extent to which the information is protected by security measures such as encryption;

IV. The kind of persons who have obtained, or could obtain, the information; and

V. The nature of the harm an individual could suffer, taking into consideration whether the individual could suffer physical, psychological, emotional, financial or reputational harm.

4. REMEDIAL ACTION

In the event that the CSO or a parish school is involved in a data breach, and action is taken in relation to the breach before it results in serious harm to any of the individuals to whom the information relates (and a reasonable person would conclude that the breach would or be likely to result in serious harm to any of the individuals), then there will be no obligation to inform the commissioner. This might be the case where, for example, where data is emailed by mistake to a trusted business partner and the school contacts them and obtains the prompt deletion of the data.

5. ASSESSING A SUSPECTED BREACH

5.1 If the CSO or parish school has reasonable grounds to suspect a data breach may have occurred, it is required to carry out a reasonable and timely assessment to ascertain whether a breach did in fact occur.

5.2 The CSO or parish school must take reasonable steps to ensure that the assessment is completed within 30 days of becoming aware of the suspected breach.

5.3 After assessing that there has been a data breach, the Data Breach Response Team must be notified.

6. NOTIFYING THE COMMISSIONER

6.1 If the Data Breach Response Team is made aware that there are reasonable grounds to believe that there has been a notifiable data breach, it is required as soon as practicable to provide a statement to the Commissioner that sets out the following:

I. The CSO or parish school's contact details;

II. A description of the data breach reasonably believed to have happened;

III. The kind of information concerned; and

IV. Recommendations about steps that individuals should take in response to the breach, for example, if a file containing parents' credit card details was hacked into, the school might recommend that the parents cancel their credit cards.

6.2 If it is then practicable to do so, the CSO or parish school must notify the contents of the statement to each of the individuals affected by the breach. In the event that a notifiable breach affects students, it will be appropriate to notify parents/carers instead of notifying students directly.

6.3 If it is not practicable to notify each individual, a more general notice may be published, such as on the CSO or school's website.

7. DATA BREACH RESPONSE PLAN

7.1 As there is an obligation under the Privacy Act for the CSO and parish schools to take reasonable steps to protect the personal information held by them from misuse, interference and loss, and from unauthorised access, modification or disclosure, one of the reasonable steps that to be taken is the preparation and implementation of a data breach response plan.

7.2 The key steps in responding to a data breach or suspected data breach are as follows:

I. Contain the breach and conduct a preliminary assessment;

II. Evaluate the risks associated with the breach;

III. Notification; and

IV. Prevent future breaches.

Each of the steps are set out further below.

8. CONTAIN THE BREACH AND CONDUCT A PRELIMINARY ASSESSMENT

8.1 As soon as a data breach or suspected data breach is discovered, immediate steps must be taken to limit the breach, including the following:

I. Contain the breach - Take the necessary steps to immediately contain the breach. For example, stop the unauthorised practice, recover the records or shut down the system that was breached. If it is not practicable to shut down a system or if it would result in the loss of evidence, then revoke or change computer access privileges or address the weakness in physical or electronic security. Also assess whether steps can be taken to mitigate the harm an in individual may suffer as a result of the breach.

II. Conduct a preliminary assessment – The Data Breach Response Team should conduct the initial investigation, gather any necessary information and make initial recommendations. If necessary, a more detailed evaluation may subsequently be required. The following preliminary aspects should be considered:

- 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?

III. Consider who needs to be immediately notified - Determine who needs to be made aware of the breach (internally, and potentially externally) at this preliminary stage. In some cases it may be appropriate to notify the affected individuals immediately (for example, where there is a high level of risk of serious harm to affected individuals). If the breach appears to involve theft or other criminal activity, it will generally be appropriate to notify the police. If the data breach is likely to involve a real risk of serious harm to individuals, or receive a high level of media attention, inform the OAIC. The OAIC may be able to provide guidance and assistance.

IV. Where a law enforcement agency is investigating the breach, consult the investigating agency before making details of the breach public. Be careful not to destroy evidence that may be valuable in determining the cause or would allow the agency or organisation to take appropriate corrective action. Ensure appropriate records of the suspected breach are maintained, including the steps taken to rectify the situation and the decisions made.

9. EVALUATE THE RISKS ASSOCIATED WITH THE BREACH

9.1 In order to determine further steps that are immediately necessary, risks associated with the breach must be assessed. The following factors should be taken into consideration:

I. The type of personal information involved:

- Does the type of information that has been compromised create a greater risk of harm?
- Who is affected by the breach?

II. The context of the affected information and the breach:

- What is the context of the personal information involved, for example the sensitivity of personal information that may also be publicly available information, or the implication of an association with the CSO or parish school?
- What parties have gained unauthorised access to the affected information, for example employee records containing information concerning performance and disciplinary matters may be particularly sensitive if exposed to other employees in the workplace?
- Have there been other breaches that could have a cumulative effect, such as separate breaches that might not, by themselves, be assessed as representing a real risk of serious harm to an affected individual, may meet this threshold when the cumulative effect of the breaches is considered.
- How could the personal information be used, for example could the information be used for fraudulent or otherwise harmful purposes, such as to cause significant embarrassment to the affected individual, or could the compromised information be easily combined either with other compromised information or with publicly available information to create a greater risk of harm to the individual?

III. Establish the cause and extent of the breach:

- Is there a risk of ongoing breaches or further exposure of information, for example what was the extent of the unauthorised access to or collection, use or disclosure of personal information, including the number and nature of likely recipients and the risk of further access, use or disclosure, including via mass media or online?
- Is there evidence of theft, and is there evidence that the information was the target of the theft, for example if a laptop computer was stolen, can it be determined if the thief wanted the information on the laptop, or the laptop hardware itself?
- Was the personal information adequately encrypted or otherwise not easily accessible, for example is the information rendered unreadable by security measures that protect the stored information, or is the personal information displayed or stored in such a way so that it cannot be used if breached? If an investigation shows that information

- on a stolen laptop was not accessed, copied or otherwise tampered with, notification to affected individuals may not be necessary.
- What was the source of the breach, for example, did the breach involve external or internal malicious behaviour, or was it an internal processing error? Does the information seem to have been lost or misplaced? The risk of harm to the individual may be less where the breach is unintentional or accidental, rather than intentional or malicious.
- Has the personal information been discovered, for example has a lost laptop been found or returned, and if information has been recovered, are there any signs that it has been accessed, copied or otherwise tampered with?
- What steps have been taken to mitigate the harm, for example have compromised security measures such as passwords been replaced? Has the full extent of the breach been assessed? Are further steps required?
- Was the breach a result of a systematic problem or an isolated incident? When checking the source of the breach, it is important to check whether any similar breaches have occurred in the past.
- How many individuals are affected by the breach? If the breach is a result of a systemic problem, there may be more people affected than first anticipated. Even where the breach involves accidental and unintentional misuse of information, if the breach affects many individuals, the scale of the breach may create greater risks that the information will be misused. The response should be proportionate.

IV. Assess the risk of harm to the affected individuals:

- Who is the recipient of the information? Is there likely to be any relationship between the unauthorised recipients and the affected individuals or was the recipient a trusted, known entity or person that would reasonably be expected to return or destroy the information without disclosing or using it?
- What harm to individuals could result from the breach, including identity theft, financial loss, threat to physical safety, threat to emotional wellbeing, loss of business or employment opportunities, humiliation, damage to reputation or relationships or workplace or social bullying or marginalisation?

V. Assess the risk of other harms:

- Loss of public trust;
- Reputational damage;
- Loss of assets such as stolen computers or storage devices;
- Financial exposure, for example if bank account details are compromised;

- Regulatory penalties, for example for breaches of the Privacy Act;
- Extortion; or
- Legal liability.

10. NOTIFICATION

10.1 In the first instance, all suspected data breaches must be notified to the CSO Data Breach Response Team.

10.2 While notification is an important mitigation strategy, it will not always be an appropriate response to a breach. Providing notification about low risk breaches can cause undue anxiety and de-sensitise individuals to notice. Each incident needs to be considered on a case-by-case basis to determine whether breach notification is required.

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

10.4 In assessing the need to notify individuals, after taking into consideration the particular circumstances of the breach, the following should be taken into account:

I. What is the risk of harm to the individual?

II. What is the ability of the individual to avoid or mitigate possible harm if notified of a breach?

III. Even if the individual would not be able to take steps to fix the situation, is the information that has been compromised sensitive, or likely to cause humiliation or embarrassment for the individual?

IV. What are the legal and contractual obligations to notify, and what are the consequences of notification?

10.5 There may be adverse consequences if an agency or organisation does not notify affected individuals. For example, if the public, including the affected individuals, subsequently find out about the breach through the media, there may be loss of public trust in the agency or organisation (which, in turn, could have its own costs).

10.6 **Notification process**

At this stage, there should be a complete set of facts as possible and a risk assessment completed to determine whether to notify individuals. The following set out some of the considerations in the notification process.

10.7 Sometimes the urgency or seriousness of the breach dictates that notification should happen immediately, before having all the relevant facts.

10.8 **When to notify –** The appropriate time frames to notify individuals are as follows**:**

I. In general, individuals affected by the breach should be notified as soon as reasonably possible;

II. If law enforcement authorities are involved, check with those authorities whether notification should be delayed to ensure that the investigation is not compromised; and

III. Delaying the disclosure of details about a breach of security or information systems may also be appropriate until that system has been repaired and tested or the breach contained in some other way.

10.9 **How to notify –** appropriate methods of notification are as follows:

I. In general, the recommended method of notification is direct, by phone, letter, email or in person to the affected individuals.

II. Indirect notification, either by website information, posted notices, media, should generally only occur where direct notification could cause further harm, is cost-prohibitive, or the contact information for affected individuals is not known.

III. Preferably, notification should be 'standalone' and should not be 'bundled' with other material unrelated to the breach, as it may confuse recipients and affect the impact of the breach notification.

IV. In certain cases, it may be appropriate to use multiple methods of notification.

V. Agencies and organisations should also consider whether the method and content of notification might increase the risk of harm, such as by alerting the person who stole the laptop of the value of the information on the laptop, if it would not otherwise be apparent.

VI. To avoid being confused with 'phishing' emails, email notifications may require special care. For example, only communicate basic information about the breach, leaving more detailed advice to other forms of communication.

10.10 **Who should provide the notification –** notifications to individuals should be provided as follows:

I. Typically, the agency or organisation that has a direct relationship with the customer, client or employee should notify the affected individuals. This includes where a breach may have involved handling of personal information by a third party service provider, contractor or related body corporate.

II. Joint and third party relationships can raise complex issues. For example, the breach may involve information held by a third party 'cloud' data storage provider, based outside of Australia. Does the agency or organisation that suffered the breach have contact details for the affected individuals? Are they able to obtain them easily? Or could they draft and sign off the notification, for the lead organisation to send?

10.11 **Who should be notified –** those that should be notified are as follows:

I. Generally, it should be the individual(s) affected by the breach. However, in some cases it may be appropriate to notify the individual's guardian or authorised representative on their behalf.

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

III. Where appropriate, clinical judgement may be required where notification may exacerbate health conditions, such as acute paranoia.

10.12 **What should be included in the notification –** The content of notifications will vary depending on the particular breach and the notification method. In general, the information in the notice should help the individual to reduce or prevent the harm that could be caused by the breach. Notifications should include the types of information as follows:

I. **Incident Description —** Information about the incident and its timing in general terms. The notice should not include information that would reveal specific system vulnerabilities.

II. **Type of personal information involved —** A description of the type of personal information involved in the breach. Be careful not to include personal information in the notification, to avoid possible further unauthorised disclosure.

III. **Response to the breach —** A general account of what the has been done to control or reduce the harm, and proposed future steps that are planned.

IV. **Assistance offered to affected individuals —** What the agency or organisation will do to assist individuals and what steps the individual can take to avoid or reduce the risk of harm or to further protect themselves.

V. **Other information sources —** Sources of information designed to assist individuals in protecting against identity theft or interferences with privacy. For example, guidance on the OAIC's website at www.oaic.gov.au and the Attorney-General's Department website at www.ag.gov.au/www/agd/agd.nsf/page/Crimeprevention_Identitysecurity.

VI. **CSO or parish school contact details —** Contact information of areas or personnel within the agency or organisation that can answer questions, provide further information or address specific privacy concerns.
Where it is decided that a third party will notify of the breach, a clear explanation should be given as to how that third party fits into the process and who the individual should contact if they have further questions.

VII. **Whether breach notified to regulator or other external contact(s) —** Indicate whether the OAIC or other parties have been notified.

VIII. **Legal implications —** The precise wording of the notice may have legal implications; consideration should be given to whether legal advice should be sought. The legal implications could include secrecy obligations that apply to agencies.

IX. How individuals can lodge a complaint with the agency or organisation — Provide information on internal dispute resolution processes and how the individual can make a complaint to the agency or organisation or industry complaint handling bodies

X. **How individuals can lodge a complaint with the OAIC** —Explain that if individuals are not satisfied with the response by the CSO or parish

school to resolve the issue, they can make a complaint to the OAIC. The OAIC's contact details are set out at page 39.

10.13 **Who else should be notified -** In general, notifying the OAIC, or other authorities or regulators should not be a substitute for notifying affected individuals. However, in some circumstances it may be appropriate to notify the following third parties:

I. **OAIC —** The OAIC strongly encourages agencies and organisations to report serious data breaches to the OAIC.

II. The following factors should be considered in deciding whether to report a breach to the OAIC:

- any applicable legislation that may require notification;
- the type of the personal information involved and whether there is a **real risk of serious harm** arising from the breach, including non-monetary losses;
- whether a large number of people were affected by the breach;
- whether the information was fully recovered without further disclosure;
- whether the affected individuals have been notified; and
- if there is a reasonable expectation that the OAIC may receive complaints or inquiries about the breach.

III. **Police —** If theft or other crime is suspected. The Australian Federal Police should also be contacted if the breach may constitute a threat to national security.

IV. **Insurers or others —** If required by contractual obligations.

V. **Credit card companies, financial institutions or credit reporting agencies —** If their assistance is necessary for contacting individuals or assisting with mitigating harm.

VI. **Professional or other regulatory bodies —** If professional or regulatory standards require notification of these bodies. For example, other regulatory bodies, such as the Australian Securities and Investments Commission, the Australian Competition and Consumer Commission, and the Australian Communications and Media Authority have their own requirements in the event of a breach.

VII. **Other internal or external parties not already notified —** The CSO and parish schools should consider the potential impact that the breach and notification to individuals may have on third parties, and take action accordingly. For example, third parties may be affected if individuals cancel their credit cards, or if financial institutions issue new cards. Consider:

- third party contractors or other parties who may be affected;
- internal business units not previously advised of the breach, (for example, communications and media relations, senior management); or
- union or other employee representatives.

VIII. **Agencies that have a direct relationship with the information lost/stolen —** Agencies and organisations should consider whether an incident compromises Australian Government agency identifiers such as TFNs or Medicare numbers. Notifying agencies such as the Australian Taxation Office for TFNs or Medicare Australia for Medicare card numbers may enable those agencies to provide appropriate information and assistance to affected individuals, and to take steps to protect the integrity of identifiers that may be used in identity theft or other fraud.

11. PREVENT FUTURE BREACHES

11.1 Once the immediate steps are taken to mitigate the risks associated with the breach, the CSO or parish schools need to take the time to investigate the cause and consider whether to review the existing prevention plan or, if there is no plan in place, develop one. A prevention plan should suggest actions that are proportionate to the significance of the breach, and whether it was a systemic breach or an isolated event.

11.2 A breach prevention plan may include the following:

I. a security audit of both physical and technical security

II. a review of policies and procedures and any changes to reflect the lessons learned from the investigation, and regular reviews after that (for example, security, record retention and collection policies)

III. a review of employee selection and training practices, and

IV. a review of service delivery partners (for example, offsite data storage providers).

11.3 Further preventative steps may include the following:

I. whether and in what circumstances (and by which staff), personal information is permitted to be removed from the office, whether it is removed in electronic form on DVDs, USB storage devices such as memory sticks, portable computing devices such as laptops, or in paper files; and

II. whether their stored data, both in the office and when removed from the office, requires security measures such as encryption and password protection.

12. REPORTING A DATA BREACH TO THE AUSTRALIAN INFORMATION COMMISSIONER

12.1 The CSO Data Breach Response Team will be responsible for reporting any data breach to the OAIC. Agencies and organisations are strongly encouraged to notify the OAIC of a data breach where the circumstances indicate that it is appropriate to do so. The potential benefits of notifying the OAIC of a data breach may include the following:

I. The CSO's decision to notify the OAIC on its own initiative is likely to be viewed by the public as a positive action. It demonstrates to clients and the public that the agency or organisation views the protection of personal information as an important and serious matter, and may therefore enhance client/public confidence in the agency or organisation;

II. It can assist the OAIC in responding to inquiries made by the public and managing any complaints that may be received as a result of the breach. If the agency or organisation provides the OAIC with details of the matter and any action taken to address it, and prevents future occurrences, then, based on that information, any complaints received may be able to be dealt with more quickly. In those circumstances, consideration will need to be given to whether an individual complainant can demonstrate that they have suffered loss or damage, and whether some additional resolution is required. Alternatively, the OAIC may consider that the steps taken have adequately dealt with the matter; and

III. Reporting a breach does not preclude the OAIC from receiving complaints and conducting an investigation of the incident (whether in response to a complaint or on the Commissioner's initiative).

11.2 Any notice provided to the OAIC should contain similar content to that provided to individuals. It should not include personal information about the affected individuals. It may be appropriate to include the following:

I. A description of the breach

II. The type of personal information involved in the breach

III. What response the agency or organisation has made to the breach

IV. What assistance has been offered to affected individuals

V. The name and contact details of the appropriate contact person; and

VI. Whether the breach has been notified to other external contact(s).

11.3 The OAIC can be contacted as follows:

Telephone
1300 363 992 (local call cost, but calls from mobile and payphones may incur higher charges)

TTY
1800 620 241 (this number is dedicated for the hearing impaired only, no voice calls)

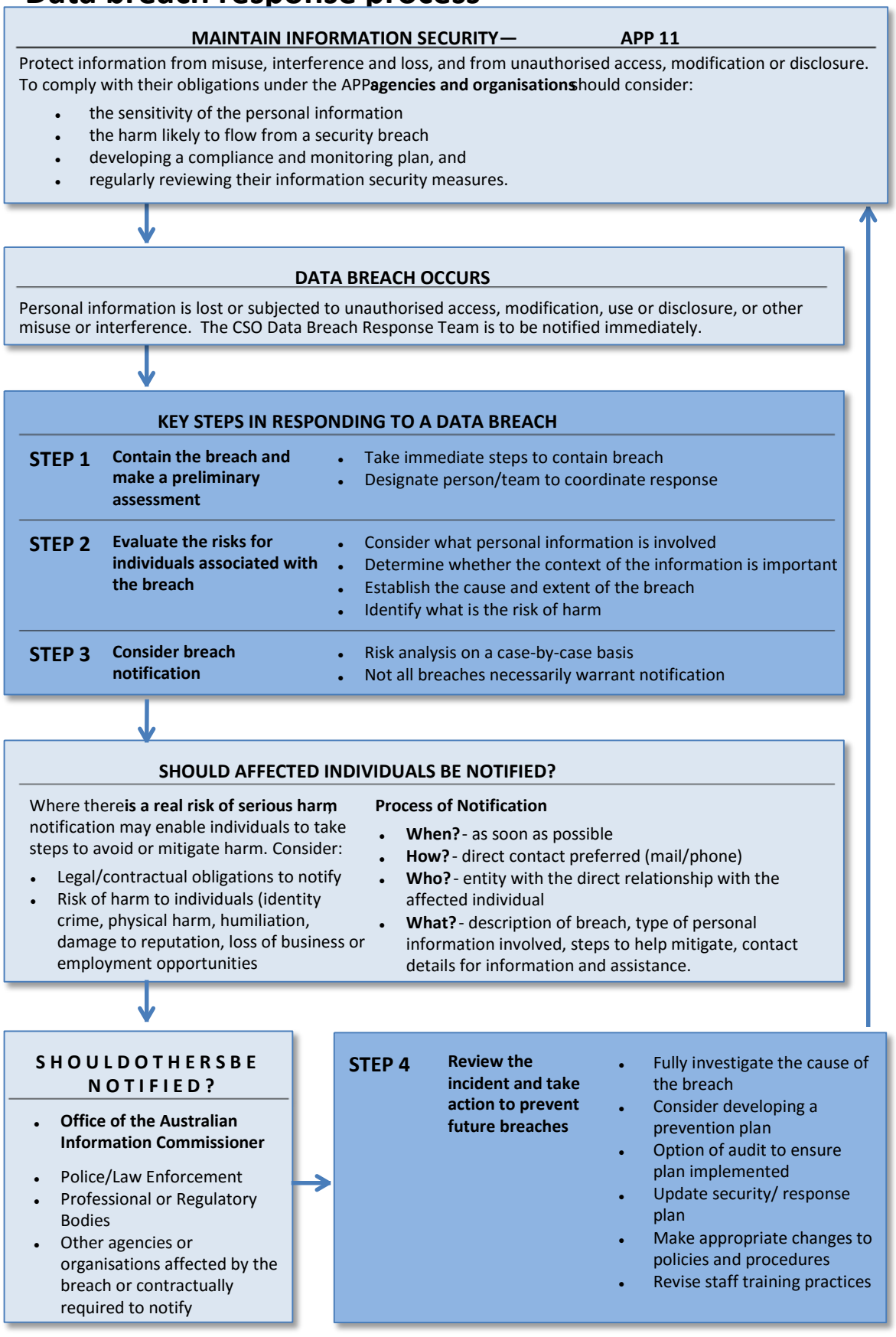
Post:
GPO Box 5218
Sydney NSW 2001

Facsimile
+61 2 9284 9666

Email
enquiries@oaic.gov.au

Website
www.oaic.gov.au

Data breach response process



VERSION HISTORY

Version	Approval Date	Authorised By	Notes
1	February 2018	Assistant Director – School Resources Services	Originally released