BUNBURY REGIONAL COMMUNITY COLLEGE

BRCC DATA BREACH RESPONSE PLAN

Contents

1. Purpose

Amendments to the *Privacy Act 1988* (Cth) in February 2018 by the Australian Government introduced the Notifiable Data Breach (NDB) scheme. The NDB scheme is a requirement developed for all agencies and organisations that are regulated under the *Privacy Act 1988*.

The scheme introduced responsibilities for organisations that handle personal information to have a procedure and structure in place to address data breaches promptly (Data Breach Response Plan) in order to reduce the risk of serious harm to individuals whose information was, or may be, disclosed.

A data breach occurs when personal information stored by an organisation is lost or subjected to unauthorised access or disclosure. Not every data breach requires compliance. Only those data breaches involving personal information that are likely to cause serious harm to any person affected require NDB scheme compliance. The NDB scheme calls them "eligible data breaches" or "notifiable data breaches".

Examples of a qualifying data breach include:

- A database with personal information is hacked
- Personal information is provided to the wrong person by mistake
- A device containing customers' personal information is stolen or lost

Where an organisation is unable to prevent the data breach from giving rise to a risk of serious harm to individuals (and the definition of "harm" includes financial, psychological, reputational and physical harm), the organisation must notify the affected individuals and the Office of the Australian Information Commissioner (OAIC).

The Australian government has created two guides for action in the occurrence of a breach

https://www.oaic.gov.au/privacy/guidance-and-advice/data-breach-preparation-and-response

https://www.oaic.gov.au/privacy/data-breaches/

Under section 26WE of the Privacy Act, a NDB occurs when:

- there is an unauthorised access or unauthorised disclosure of information, and a reasonable person would conclude that access or disclosure would be likely to result in serious harm to any of the individuals to whom the information relates; or
- information is lost in circumstances where such unauthorised access or disclosure is likely to occur and a reasonable person would conclude that, assuming such access or disclosure did occur, it would be likely to result in serious harm to any individuals to whom that information relates.

Organisations are required to notify the individuals and the OAIC within 30 days of becoming aware of the breach.

2. Scope

This policy applies to all employees of Bunbury Regional Community College.

3. Definitions

Data breach is the intentional or unintentional release of secure or private/confidential information to an untrusted environment

Phishing Phishing attacks are the practice of sending fraudulent communications that

appear to come from a reputable source. It is usually done through email. The goal is to steal sensitive data like credit card and login information, or to install malware on the victim's machine.

4. Policy

Background information

The Office of the Australian Information Commissioner (OAIC) is an independent agency within the Attorney-General's portfolio. Their primary functions are privacy, freedom of information and government information policy. When an organisation or agency the Privacy Act 1988 covers has reasonable grounds to believe an eligible data breach has occurred, they must promptly notify any individual at risk of serious harm. They must also notify the OAIC.

Under the Notifiable Data Breaches scheme, an organisation or agency that must comply with Australian privacy law has to tell individuals if a data breach is likely to cause them serious harm.

Examples of serious harm include:

- identity theft, which can affect your finances and credit report
- financial loss through fraud
- a likely risk of physical harm, such as by an abusive ex-partner
- serious psychological harm
- serious harm to an individual's reputation

The OAIC *Notifiable Breaches Quarterly Statistics Report for July - September 2018*

showed that:

1. 92 (37%) of the 245 reported data breaches were attributable to human error;
2. these human error breaches predominantly included unauthorised disclosures via verbal communications, failure to redact information, unintended publication of information, and information sent to the wrong recipient; and
3. many of the breaches attributable to malicious or criminal attacks also involved an element of human error whereby the perpetrator targeted and exploited vulnerabilities due to the involvement of a human factor (for example, an individual clicking on an attachment to a phishing email).

Accordingly, of the 245 total breaches, the majority can be said to have involved at least some element of human error.

This data is useful as it identifies some of the key areas in which BRCC can direct attention for the purposes of reducing the risks associated with in operating in an era of tighter regulation.

No amount of training or security safeguards will eliminate the risk of data breaches caused by human error.

Taking practical measures to prevent breaches is important. Ensuring that BRCC has compliant privacy policies and practices, and that all staff are adequately trained, may help prevent a notifiable data breach.

The potential consequences for failing to report a notifiable data breach are serious. Such a

failure is considered an interference with the privacy of individuals which can attract civil penalties of up to $2.1 million.

BRCC Obligations

The NDB scheme was introduced in February 2018 with the intention of embedding the privacy obligations mandated in the Privacy Act and the Australian Privacy Principles.

The key requirements under the NDB scheme are that schools must:

- have a Data Breach Response Plan in place
- report any breach to affected individuals and the OAIC.

BRCC may notify any affected individuals about a data breach by an email, text message or phone call. The notification will include:

- BRCCs name and contact details
- the kinds of personal information involved in the breach
- a description of the data breach
- recommendations for the steps that can be taken in response to the breach.

If BRCC isn't able to contact everyone they need to, they will put the data breach notification on their website. BRCC are required to promote this data breach notification, for example, through social media, news articles or advertisements.

BRCC, once aware of a NDB, must also prepare a statement in accordance with the *Privacy Act* and provide it to the OAIC, containing:

- BRCC's details and contact information
- the circumstances of the data breach
- what BRCC have done to contain the data breach
- details of any remedial action taken.

The Online form link to report the data breach is available at:https://forms.business.gov.au/smartforms/servlet/SmartForm.html?formCode=OAIC-NDB

Affected parties must be notified under the Privacy Act unless here is an exception available under sections 26WN or 26WP of the Act.

Common causes of Notifiable Data Breaches

The main cause of NDBs in the education sector according to the OIAC is human error:

- sending emails to the wrong person containing personal information
- unintentionally releasing or publishing personal information
- failing to use bcc in group emails.

Prevention of NDBs

BRCC needs to identify the personal information that the College collects and holds, then review the measures in place to protect it.

> *APP 11 requires organisations to take reasonable steps to protect the personal information they hold from misuse, interference and loss, as well as unauthorised access, modification or disclosure. Protecting personal information includes considering physical security, cyber security, and awareness and training of staff. It also involves looking at the risk points where information can be accidentally disclosed* and protecting personal data on lost or stolen equipment.

It is important that all staff know who to notify as soon as they become aware of an actual or

suspected data breach. At BRCC this will be the Principal who will then notify the College Director and Board.

By ensuring notification is done straight away BRCCs increases the chance of minimising the data breach.

Urgent steps that can be taken to minimise harm is by changing passwords or notifying banks. Deactivating data remotely on a lost phone straight away can reduce or eliminate any risks of an NDB.

Due to COVID and increased flexible working arrangements, BRCC needs to continue to make sure that staff and systems are suitable to prevent NDBs. This can be achieved through training and system maintenance.

BRCC needs to ensure that staff are aware of these risks and to encourage all staff to take all possible care to avoid these risks where possible.

Posters should be placed where staff can see them and know what to do.

https://www.oaic.gov.au/assets/privacy/data-breaches/act-quickly-if-you-are-affected-by-a-data-breach-poster.pdf

Preventing data breaches

Prevention is important to help ensure data breaches are avoided. BRCC employees need to be aware of their obligations to protect data and privacy at all times.

Principle 6 of the BRCC *Code of Conduct* covers the appropriate use of electronic communication and social networking sites. Employees are required to comply with the College's *Staff Use of BRCC ICT Resources Policy* and *Social Media* Policy.

Principle 10 of the BRCC Code of Conduct (the Code) covers communication and protecting confidential information and notes College employees should be aware that there are strong legal requirements around the collection, release and privacy of information.

Staff will be held accountable for breaches of the Code and disciplinary action may be taken in respect of an employee who breaches the Code.

Important preventative measures

- Passwords for Staff/Administration Wi-Fi should not be provided to students under any circumstance. In order to protect BRCC from possible data breaches, students are only to be provided with the Student Wi-Fi password.

- All BRCC employees should make use of a strong password on all electronic equipment and phones (where emails may be accessed). In the event a phone or laptop is lost, access to BRCC data a strong password may help protect the data until steps are taken to secure the information.

- Avoid clicking on links in emails or sharing your personal information on the phone or by email, unless you're certain the organisation or agency that has contacted you is genuine. Contact the organisation or agency instead through publicly available contact details (such as the phone book or their website)

Phishing attacks are one of the most common security challenges that both individuals and companies face in keeping their information secure. Whether it's getting access to passwords, credit cards, or other sensitive information, hackers use email, social media,

phone calls, and any form of communication they can to steal valuable data.

Careless internet browsing is a leading cause of problems. If the domain of the link to which you are being directed doesn't match the purported company domain, then the link is a fake.

Links or documents sent by email should not be opened if you do not know the sender. This will help minimise the risk of phishing and a possible cyberattack that leads to a data breach. You'll be able to check to see what is or what is not legitimate by dragging your cursor over the email sender as well as any links in the email. If the links are malicious, they will likely not match up with the email or link description.

Phishing and spear phishing attacks can be delivered through corporate email, through a user's personal email that may be connected to their mobile device or through SMS messages to the user.

Regular reminders of the above information by the Principal at staff meetings is required as part of the BRCC data breach management plan.

Steps to manage a data breach

Responding to data breaches — Four key steps

Step 1: Contain the data breach to prevent any further compromise of personal information.
Step 2: Assess the data breach by gathering the facts and evaluating the risks, including potential harm to affected individuals and, where possible, taking action to remediate any risk of harm.
Step 3: Notify any affected individuals and the OAIC Commissioner if required. If the breach is an 'eligible data breach' under the NDB scheme, it may be mandatory for the entity to notify.
Step 4: Review the incident and consider what actions can be taken to prevent future breaches.

If the breach involves your contact information:

Emails – Change your account passwords, enable multi-factor authentication if you can.

Credit card or online banking – Change your online banking account passwords and PINs and tell your bank what has happened. Check your statements and report any unusual transactions straight away to your bank or financial institution. Get a copy of your credit report to see if there are any loan requests or applications that you did not make.

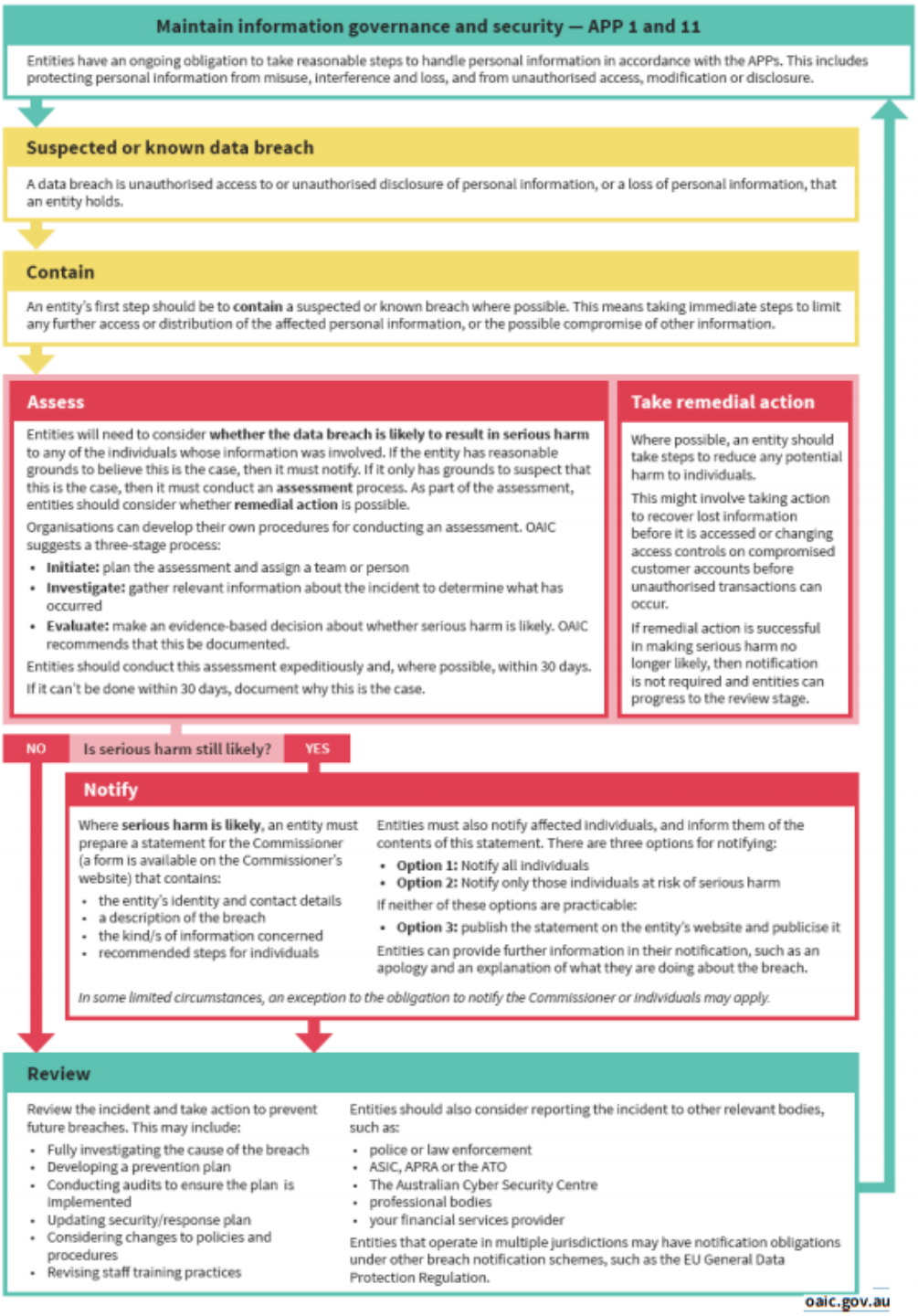
Identity documents – such as Drivers licence or Medicare card. Contact the relevant Agency for advice.

Health information – such as health care records - contact your health service provider

Tax file number – Contact the Australian Tax Office on ato.gov.au

Personal safety – If your physical safety is at risk contact the police. If you are distressed contact your doctor, family or friends, or a support service.

The following diagram summarises the data breach response process. The parts of this process that are required by the NDB scheme are coloured red.



Related Legislation and Policies

Privacy Act 1988 (Cth)
Code of Conduct
Privacy Policy
Staff Acceptable Use Of BRCC ICT Resources Policy

Policy Review Date

This policy is due for review annually.

Contact BRCC

Web: http://www.brcc.org.au/contact/
Email: principal@brcc.org.au
Phone 6724 6971
Bunbury Campus: Level 1/16 Victoria Street, Bunbury
Busselton Campus: 50 Albert St, Busselton WA 6280

1. Approval Process	New Policy or Amendment	Minor Amendment or Review
Endorsed by Principal	7/10/2021	
Approved by Director	7/10/021	
Approved by Governing Council	27/10/2021	
Next Review	September 2022	

Appendix 1 - Resources

OIAC Notifiable Data Breach form – for training purposes