Data Breach Response Plan

Purpose

The College is bound by the Australian Privacy Principles (APPs) contained in the Commonwealth Privacy Act.

The Notifiable Data Breaches (NDB) scheme under Part IIIC of the *Privacy Act 1988* took effect on 22 February 2018. The NDB Scheme requires entities governed by the Privacy Act and the APPs to notify the Office of the Australian Information Commissioner (OAIC) and the affected person/s of an eligible data breach (or NDB).

This Data Breach Response Plan sets out procedures for Bayside Christian College staff to follow in the event that the College experiences a data breach (or suspects that a data breach has occurred). The plan is a key element in ensuring the College meets its obligations under the Privacy Act.

Scope

As an attachment to the College Privacy Policy, the Data Breach Response Plan applies to students and their parents and/or guardians ('Parents'), job applicants, staff members, volunteers, contractors, Board and Association members; and all other people who come into contact with the College.

Definitions

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 and organisations.

According to the Privacy Act, an **eligible data breach** happens if:

a) there is unauthorised access to, unauthorised disclosure of, or loss of, personal information held by an entity; and
b) the access, disclosure or loss is likely to result in serious harm to any of the individuals to whom the information relates.

The phrase **likely to occur** means the risk of serious harm to an individual is more probable than not (rather than possible). In the context of a data breach**, serious harm** could include 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 in the entity's position would identify as a possible outcome of the data breach.

Unauthorised access of personal information occurs when personal information that an entity holds is accessed by someone who is not permitted to have access. This includes unauthorised access by an employee of the entity, or an independent contractor, as well as unauthorised access by an external third party (such as by hacking).

Unauthorised disclosure occurs when an entity, whether intentionally or unintentionally, makes personal information accessible or visible to others outside the entity, and releases that information from its effective control in a way that is not permitted by the Privacy Act. This includes an unauthorised disclosure by an employee of the entity.

Loss refers to the accidental or inadvertent loss of personal information held by an entity, in circumstances where is it is likely to result in unauthorised access or disclosure.

Examples of circumstances which may meet the criteria of an eligible data breach include when:

- a College device containing the personal information of students is lost or stolen,
- an unsecured device is accessed by unauthorised personnel (i.e. not locking the screen/logging out when away or through poor password security),
- a database containing personal information is maliciously accesses (e.g. hacked),
- personal information about students or staff is mistakenly provided to the wrong person (e.g. emailing student results to another parent),
- records containing student information are stolen from unsecured recycling bins or from staff pigeon holes, or
- disclosing personal information about students/staff for purposes other than what it was collected for and without the consent of the affected students/staff.

Procedural Steps

All data breaches, actual and suspected, should be reported to the College Privacy Officer and College Principal for initial assessment of whether they should be forwarded to the full Data Breach Response Team comprising:

- Executive Leadership Team – Principal, Deputy Principal & Business Manager
- Privacy Officer
- ICT Manager
- E-Learning Coordinator.

The College Privacy Officer is to keep a record of all data breaches, whether eligible or not, and all deliberations and decisions of the Data Breach Response Team.

The Data Breach Response Team Data undertakes the following procedures for breaches forwarded to it:

Step 1: Contain the breach & do a preliminary assessment

- As soon as practicable after notification of the breach, convene a meeting of the Data Breach Response Team.
- Immediately contain breach by securing ICT or physical infrastructure.
- Ensure evidence is preserved that may be valuable in determining the cause of the breach, or allowing the College to take appropriate corrective action.
- Consider developing communications strategy to manage the expectations of the internal and external community.

Step 2: Evaluate the risks associated with the breach

Investigate the breach, promptly collecting the following:

- 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 the affected individuals, or possible affected individuals
- the risk of serious harm to the affected individuals
- the risk of other harms.

Step 3: Notification

- Determine who needs to be made aware of the breach, both internally, and potentially externally.
- Determine whether to notify affected individual/s – is the access, disclosure or loss likely to result in serious harm to the individual/s to whom the information relates?
- Consider what organisations should be notified, including police/law enforcement and the OAIC (in the prescribed format).

Step 4: Prevent future breaches

- Update security (ICT or physical) and Data Breach Response Plan if necessary.
- Make appropriate changes to policies and procedures if necessary.
- Revise staff training practices if necessary.
- Review record of data breach to ensure outcomes have been actioned.

Related Policies

Staff Device Policy
Staff Password Policy

Document Version 1 – February 2018