Information Security Policy

Policy Classification		
Policy Number:	**Date of Origin:** February 2018	**Modification History:** Nil
Date of most recent review: Nil	**By Whom & Position:** Policy Review Committee	**Commencement Date:** 2018
Policy Audience: Oaklife	**Policy Status:** New	**Policy Review Date:** 2020
Policy Approval: This policy was approved by the Senior Leadership Team and Board February 2018.		
This policy supersedes all previous policies relating to matters contained herein.		

1.0 Rationale

1.1 The purpose of the Information Security policy is to set out the security requirements that Oakhill College must meet in order to manage the Confidentiality, Integrity, Availability and Privacy of Oakhill College owned data and information and the associated policies and procedures related to data breach and mandatory data breach reporting.

1.2 Data, Information and the underlying technology systems are essential assets to Oakhill College and provide vital resources to staff and students and consequently need to be suitably protected.

1.3 Information security is achieved by implementing a suitable set of controls (based on risk profile), including policies, processes, procedures, organisational structures and software and hardware functions.

1.4 Oakhill College is committed to providing a secure, yet open information environment that protects the confidentiality, integrity, of information without compromising access and availability.

2.0 Guiding Principles

The following principles outline the minimum standards that guide the College's Information Security processes and procedures and must be adhered to by all members of the College community.

2.1 This Information Security Policy defines the principles for establishing effective security measures to ensure the confidentiality, integrity, availability and privacy of information collected, shared, and stored.

2.2 The Information Security Policy covers:

1. Information assets in electrical, paper, audio or video form.
2. The continued availability of information and the entire information environment to support activities, including the implementation of appropriate controls to protect information from intentional or accidental disclosure, manipulation, modification, removal or copying.
3. Information held and maintained for the College by external parties
4. Information held by the College on behalf of external parties
5. All staff fulltime, casual, temporary or contractors.
6. All processes and operations
7. All locations where College information is stored either permanently or temporarily. This includes but is not restricted to all College worksites, non-College worksites such as private residences, and mobile devices
8. ICT infrastructure owned or leased by the College and any ICT connecting to it or residing on the College's ICT infrastructure
9. Data breach and mandatory reporting of data breach procedures.

3.0 Policy

3.1 Oakhill College Responsibilities

Oakhill College is responsible for safeguarding the College Information Environment and Information Resources against security threats. The College discharges its responsibilities through the following:

1. Defining roles and responsibilities and establishing clear lines of accountability;
2. Protecting the College's information assets against internal and external threats (e.g. security breach, loss of data);
3. Ensuring that the College complies with applicable laws, regulations, and standards;
4. Identifying and treating security risks to the College's information environment through appropriate physical, technical and administrative channels; and
5. Implementing an Information Security Management System (ISMS) in accordance with the following Standards for information security:

- ISO/IEC 27001 ISMS Requirements
- ISO/IEC 27002 ISMS Code of Practice

6. Assigning a Chief Information Officer (CIO) to implement, manage and maintain the College ISMS.
7. To limit access to information and information processing facilities
8. To establish and maintain the protocol for using digital messaging in all its forms including security aspects of information transfer
9. To ensure the protection of information and the secure operation of networks and supporting processes.
10. To prevent unauthorised physical access, damage and interference to the college information facilities.
11. To ensure protection of the College's information assets that are accessible to service providers
12. To ensure a consistent an effective approach to the management of information security incidents
13. To avoid breaches of legal, statutory, regulatory or contractual obligations to information security

3.2 User Responsibilities

1. Users must abide by all relevant laws and policies of the College regarding information security and data breach.
2. Users are expected to take responsibility for developing an adequate level of information security awareness, education, and training to ensure appropriate use of the information environment.
3. Users may only access information needed to perform their authorised duties.
4. Users are expected to determine and understand the classification of the information to which access has been granted through training, other resources or by consultation with the relevant line manager.
5. Users must protect the confidentiality, integrity and availability of the College's information as appropriate for the information classification level.
6. Users may not in any way divulge, copy, release, sell, loan, alter or destroy any information, except as authorised by the relevant College delegate.
7. Users must safeguard any physical key, ID card or computer/network account that enables access to College information. This includes maintaining appropriate password creation and protection measures as set out in the password composition guidelines.
8. Any activities considered likely to compromise sensitive information or may be classified as a data breach must be reported to the Director of IT.
9. Users are obliged to protect sensitive information even after separation from the College

3.3. Managers and Supervisors

In addition to complying with the requirements listed above for all staff and contractors, managers and supervisors must:

1. Ensure that departmental procedures support the objectives of confidentiality, integrity and availability, and that those procedures are followed.
2. Ensure that restrictions are effectively communicated to those who use, administer, capture, store, process or transfer the information in any form, physical or electronic.
3. Ensure that each staff member understands his or her information security related responsibilities.

3.4 Director of IT

In addition to complying with the stated policy requirements defined for all staff, contractors, the Director of IT as system manager is responsible for:

1. Ensuring adequate security for computing and network environments that capture, store, process and/or transmit information;

2. Ensuring that the requirements for confidentiality, integrity and availability as defined by the appropriate system managers are being appropriately managed within their respective environments.
3. Understanding the classification level of the information that will be captured by, stored within, processed by, and/or transmitted through their technologies.
4. Developing, implementing, operating and maintaining a secure information environment that includes:
   a. A cohesive architecture;
   b. System implementation and configuration standards;
   c. Procedures and guidelines for administering network and system accounts and access privileges in a manner that satisfies the security requirements defined by the systems managers; and
   d. An effective strategy for protecting information against generic threats posed by computer hackers that adheres to industry-accepted "information management best practices" for the system or service.
   e. Policies and procedures relating to data breaches and mandatory reporting of data breaches.

4.0 Procedures

5.0 Policy Evaluation and Review

The College Principal is to ensure that this Policy is reviewed in 2020

6.0 Explanatory Notes and Definitions

This Section provides further detailed information to support the implementation of the Colleges *Information Security Policy*

6.1 Information

6.1.1 Definitions

Data is defined as "a collection of organised items. This may consist of numbers, words, or images, particularly as measurements or observations of a set of variables. Data generally refers to facts – it can be structured or unstructured.

Information is defined as the collection of these facts in a specific context from which conclusions can be drawn.

6.1.2. Information Types

Data requirements will vary depending on the nature and sensitivity of the Information that can be derived from the data. The College's Information may include the following (which are not mutually exclusive):

- **State Records:** Under the *State Records Act 1998 (NSW)*, '**record**' means any document or other source of information compiled, recorded or stored in written form or on film, or by electronic process, or in any other manner or by any other means. '**State record**' means any record made and kept, or received and kept, by any person in the course of the exercise of official functions in a public office, or for any purpose of a public office, or for the use of a publicoffice…''

  Information that falls under the definition of State Records must comply with the relevant *State Records* legislation.

- **Personal Information**: Under the *Privacy and Personal Information Protection Act 1998 (NSW)*, '**Personal Information**' means information or an opinion (including information or an opinion forming part of a database and whether or not recorded in a material form) about an individual whose identity is apparent or can reasonably be ascertained from the information or opinion.

  Information that falls under the definition of Personal Information must comply with the relevant privacy legislation.

- **Health Information**: Personal Information that relates to the physical or mental health or disability of an individual, or health services, may be subject to further obligations under the *Health Records and Information Privacy Act 2002 (NSW)*.

- **Public Information**: Information that has been approved for public release or is available to the public (such as through the *Government Information Public Access Act 2009 (NSW)*. Unauthorised disclosure of this information is unlikely to cause serious problems for the Department, NS Government, its customers, or its business partners.

- **Sensitive information**: Information that is considered as sensitive to the Department and classified according to the Office of Finance and Services (OFS) *DFS C2013-5 Information Classification and Labelling*.

- **Confidential information**: Information that has not been labelled as sensitive information but may be subject to confidentiality obligations. For example, it is common in commercial contracts for each party to keep the other party's confidential information (e.g. intellectual property such as source code or financial arrangements such as service fee calculations) confidential. If this Information were maintained by a service provider and there was unauthorised disclosure of this information by the service provider, the College may be in breach of its confidentiality obligations to the contractor.

- **Critical information**: Information that is critical to the College would require a high level of data integrity and availability. The failure to retrieve accurate critical Information in a timely manner would significantly impact on the Department's operations.

6.1.3. Information Security

Information Security is the protection and preservation of information including the confidentiality, integrity, and availability.

Confidentiality (including Privacy) - Ensuring that information (sensitive or private) is accessible only to those authorised to have access.

Integrity - Safeguarding the accuracy and completeness of information and processing methods.

Availability - Ensuring that authorised users have access to information and associated assets, when required.

6.2. Information is an Enterprise Asset

One of the key strategies of the College is to enhance information management to support teaching, learning, reporting and public accountability. The College manages enterprise information as an asset via an Information Security Management System that takes into account a minimum set of controls, and requirements relating to certification, attestation and the establishment of the Digital Information Security Community of Practice.

6.3 Information Security Management System

An Information Security Management System (ISMS) is the framework and methodology used by the College to manage the risks to its information assets. The ISMS is an ongoing management process which aims to continually improve security controls.

The overall objective of an ISMS is to ensure that information security risks are properly identified, and effectively and efficiently managed.

Developing an ISMS involves the following key steps:

6.3.1 Creation of a management framework for information

This sets the governance (i.e. direction and objectives) for information security and defines a policy which has organisational support and commitment. The *ISMS Framework* will be developed and will define the objectives, governance and roles and responsibilities.

6.3.2 Identification of information security requirements

The key to managing information security risks is to understand the information asset and its business significance. As a part of this process, information assets will be identified and classified according to their levels of criticality, sensitivity and risk.

An *Information Classification Standard* will be developed during the implementation of the Information Security Policy.

The *Enterprise Risk Management Guidelines* will be used to assess security risks. The results of this assessment will help determine the appropriate management action for managing the identified risks.

6.3.3 Selection and implementation of controls

Controls should be selected and implemented once security requirements have been identified. These controls need to ensure that risks are reduce to an acceptable level. The extent of implementation of controls needs to be balanced against the potential business impact that may arise from security failures.

Controls can be in the form of policies, practices, standards, procedures, guidelines, technology and organisational structures. They will vary from system to system, depending on the criticality and sensitivity of the particular information asset.

6.3.5 Evaluation of effectiveness

Security controls and procedures should be regularly evaluated to ensure they address the ongoing security requirements.

6.3.6 Continual improvement

The College will continually improve the Information Security Management System (ISMS) including information security processes, techniques and controls.

The implementation of an ISMS enables the College to demonstrate an industry best practice approach for the identification, assessment and control of security of its information.

The College may implement a comprehensive, enterprise wide ISMS, or many smaller ISMSs, each of which would have their own defined scope. An ISM may be scoped using a variety of factors:

- by information asset (e.g. staff or student records)
- by business unit (e.g. Finance)

- by process (e.g. employee screening)
- by service (e.g. Internet browsing filtering)
- by geography (e.g. North Coast Institute)
- by information system (e.g. payroll)
- by ICT infrastructure (ITD Data Centres).

An ISMS will not make the College immune from security breaches. It will, however, make the occurrence of security breaches less likely and reduce the consequential costs and disruption, if they do occur.

The College may be required to obtain Certification of the ISMS by a third party. An existing Certification Program is being managed by the Information Security Unit (ISU). Please contact ISU for further information and prior to undertaking any certification activities

6.4 Information Security Framework

The operational management of Information Security requires a number of components. Each component contains one or more Standards which are further supported by guidelines, procedures and/or checklists.

These components are displayed in Figure 1 below.

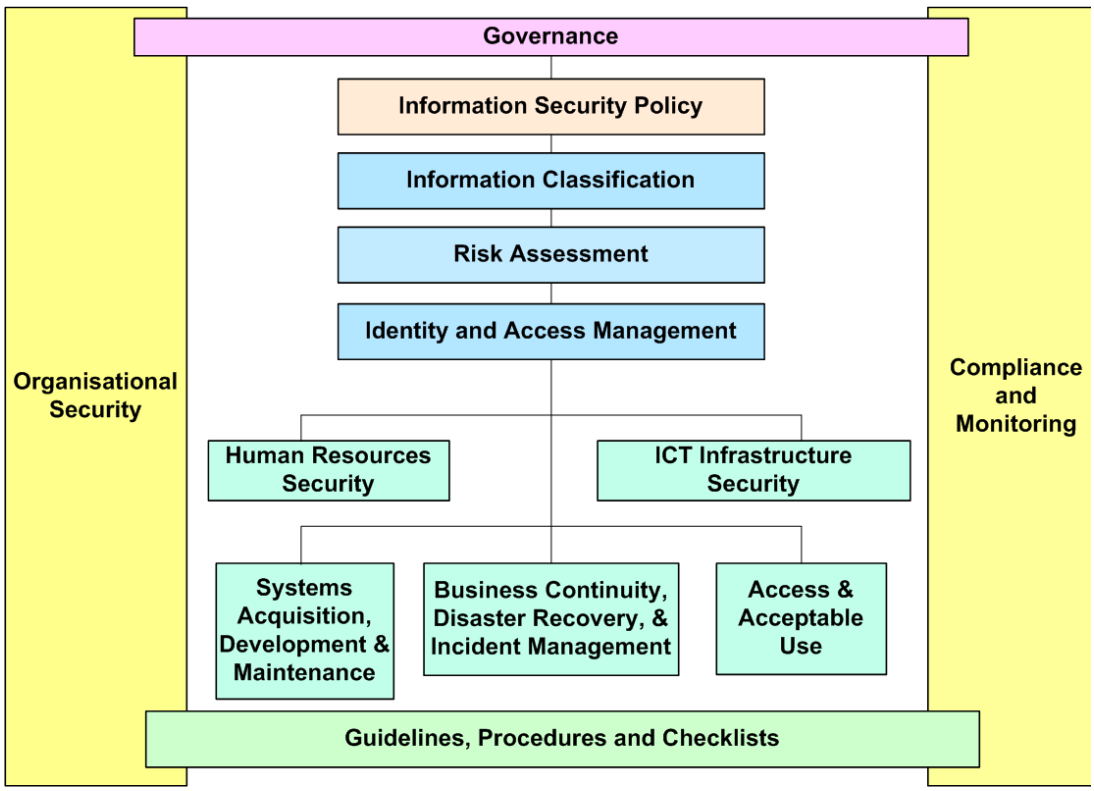


Figure 1 - Components of an Information Security Framework

The Governance framework will be developed and monitored by the Information Security Steering Committee.

6.5 Information Classification

The NSW Government 'Classification Schema' was published in the Office of Finance and Services' circular - *DFS C2013-5 Information Classification and Labelling Guidelines*.

6.6 Risk Assessment

Controls to mitigate information security risk should be selected from the information security standards, procedures and guidelines.

Risk Assessments must be performed at least annually, or under the following circumstances:

- For new system development or implementation
- As a result of significant changes to processes, facilities or operation
- Whenever a new threat is identified
- Whenever the threat landscape is considered to have increased (e.g. after a serious incident).

6.7 Identity and Access Management

The level and duration of access to an information asset or system shall be based on the:

- role of the individual accessing the information asset or system (or need to know);
- security classification of the information asset or system; and
- risk associated with the information asset or system.

6.8 Human Resources Security

All users of the College's information assets, including ICT infrastructure are responsible for familiarising themselves with and complying with the College's policies, procedures and standards. Users must ensure they access and use information assets in an approved and appropriate manner.

Users' security responsibilities should be included in:

- job/position descriptions
- contracts
- acceptable use agreements
- memoranda of understanding.

Roles that require a high degree of trust (such as systems administrators and privileged users) should undertake additional screening and/or probity assessments before employment commences.

Users should be given appropriate security awareness training to inform them of their security responsibilities and to ensure they maintain their capability to carry out these responsibilities.

6.9 Information and Communications Technology (ICT) Infrastructure Security

The College's ICT infrastructure must be securely configured, installed, administered, managed and monitored.

Information managers should ensure their systems are secured sufficiently to protect the information that they contain.

Shared infrastructure should be secured according to security requirements of the most critical system.

6.10 Access and Acceptable Use

Access should be provided only to people who have a need to know the information.

In all situations, individuals should be provided the least privilege necessary to carry out their role and/or responsibility.

All information users are responsible for their accounts or access privileges. Users should take all reasonable care to ensure that their account remains secure. The sharing of accounts is not allowed.

6.11 Systems Acquisition, Development and Maintenance

Information must be secured at each stage of its lifecycle (creation, dissemination, access, storage and disposal).

Information security requirements must be addressed, during changes or projects, to identify risks and to ensure appropriate mitigation plans are developed.

6.12 Business Continuity Planning, Disaster Recovery and Incident Management

Information security requirements should be incorporated into all business continuity and disaster recovery plans.

All remaining incidents should be managed according to standard incident management procedures.

6.13 Compliance and Monitoring

The College's *Code of Conduct* requires that all staff comply with all College policies and procedures.

Breaches or circumvention of the Information Security Policy, standards and procedures should be managed according to procedures described in the *Code of Conduct*.

The College reserves the right to monitor access and use of information assets and ICT infrastructure. Monitoring will be conducted in an ethical, consistent and objective manner, and comply with the *Workplace Surveillance Act (2005)* and the College's *Privacy Policy*.

The Director of IT will monitor the implementation and effectiveness of this policy and standards, as well as performing compliance reviews.

6.14 Responding to Data Breaches

A data breach concerns the security of personal information and involves the actual unauthorised access or disclosure of personal information, or the loss of personal information where the loss is likely to result in unauthorised access or disclosure (Data Breach).

Data Breaches are not limited to the malicious acts of third parties, such as theft or 'hacking', but may also arise from human error, a systems failure, or a failure to follow information handling or data security policies resulting in accidental loss, access or disclosure. Data Breaches are different from an interference with privacy that involves a breach of another privacy principle such as a use or disclosure of personal information which is not permitted under APP6 (see Section 9 – Use or disclosure of personal information of the 2018 NSW Catholic & Independent Schools and AIS Privacy Compliance Manual). The following are examples of when a Data Breach may occur:

- loss of smartphone or other School device or equipment containing personal information;
- cyber-attacks on the School's system, resulting in unknown third parties accessing or stealing personal information;
- accidental transmission of personal information such as student's reports to unintended recipients via e-mail;

- loss or theft of hard copy documents; and
- misuse of personal information of students or parents by School personnel.

From 22 February 2018, all agencies and organisations with existing personal information security obligations under the Privacy Act, including Schools, are required to report certain data breaches under the notifiable data breaches scheme (NDB Scheme). The NDB Scheme was inserted into the Privacy Act by the Privacy Amendment (Notifiable Data Breaches) Act 2017 (Cth). It sets out obligations to notify affected individuals and the Information Commissioner about data breaches which fall within the definition of an 'eligible data breach' (EDB).

A Data Breach is an EDB if it is likely to result in serious harm to an individual or individuals whose information is involved in the Data Breach. Not all Data Breaches will be EDBs. For example, if a School acts quickly to remediate a Data Breach, and as a result of this action the Data Breach is not likely to result in serious harm, there is no obligation to notify any individuals or the Information Commissioner. However, in some cases, a School may decide to voluntarily notify individuals and/or the Information Commissioner. There are also limited exceptions to notifying affected individuals and the Information Commissioner of an EDB in certain circumstances.

Section 26 of the 2018 NSW Catholic & Independent Schools and AIS Privacy Compliance Manual provides guidance for Schools regarding:

- containing a Data Breach;
- assessing whether a Data Breach is an EDB and taking remedial action to reduce the likelihood of harm to individuals affected by the Data Breach;
- notifying the Information Commissioner of an EDB and notifying individuals affected by an EDB, and potential exceptions to notification; and reviewing the Data Breach/EDB.

An adapted version of the OAIC Data Breach Response Summary setting out these steps is included in the Appendix.

Additional useful resources:

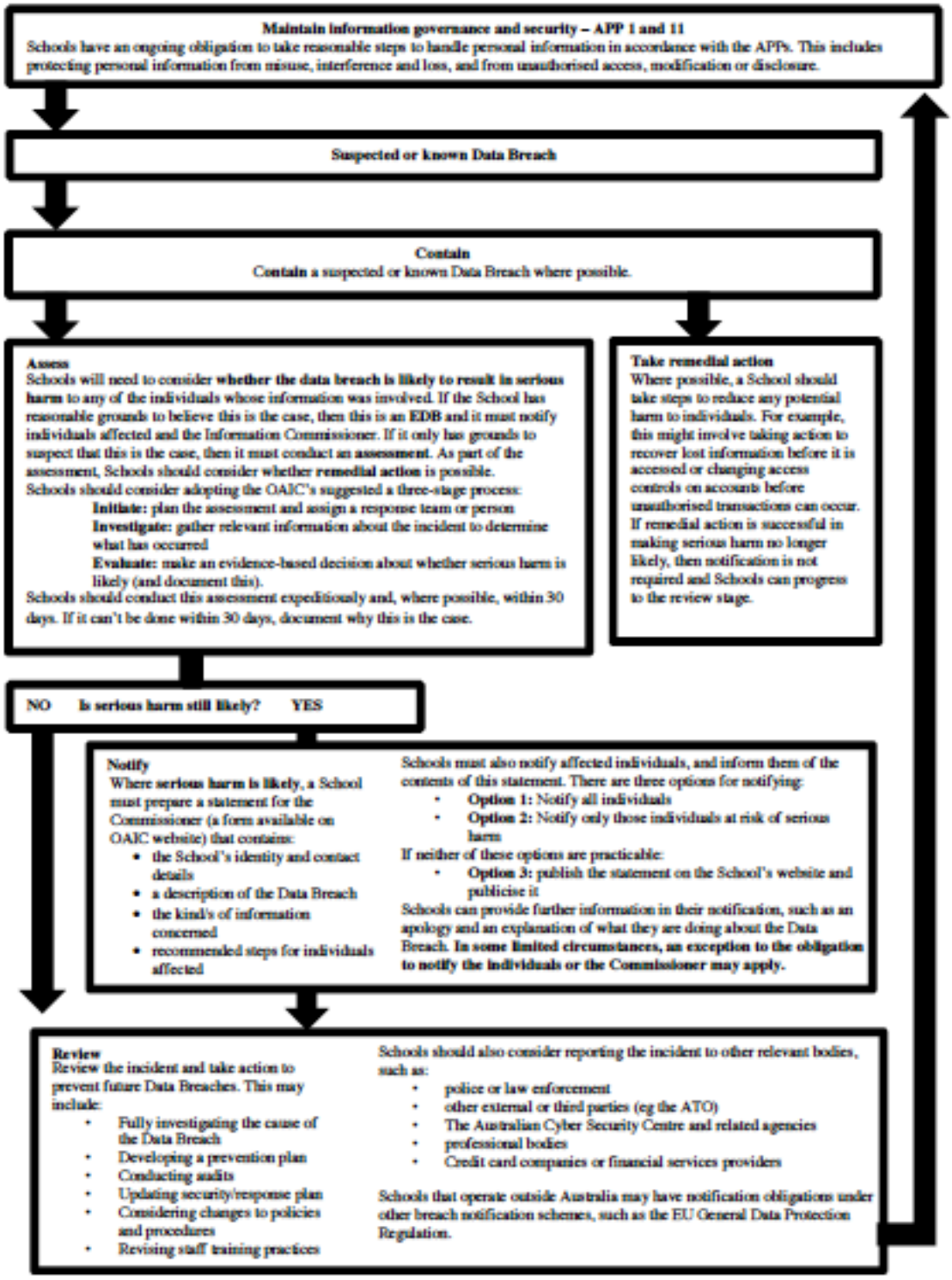
- the OAIC's NDB Scheme: Resources for agencies and organisations available at www.oaic.gov.au/privacy-law/privacy-act/notifiable-data-breaches-scheme (OAIC Resources);
- the Privacy Amendment (Notifiable Data Breaches) Act 2017 (Cth) (Amending Act); and the explanatory memorandum for the Privacy Amendment (Notifiable Data Breaches) Bill (Explanatory Memorandum).
-

7.0 Supporting and Related Documents, Procedures and Guidelines

- NSW State Records Act 1998
- NSW Privacy and Personal information Protection Act 1998
- NSW Workplace Surveillance Act 2005
- Department of Premier and Cabinet Memorandum M2012-15 Digital Information Security Policy
- National Catholic Education Commission and Independent Schools Council Australia Privacy Compliance Manual (2018)

8.0 Appendices

Appendix 1: Mandatory Notification of Eligible Breaches Summary



**This summary is a modified version of the OAIC Data Breach response summary available at www.oaic.gov.au/privacy-law/privacy-act/notifiable-data-breaches-scheme*

MT_140223174_5

Appendix 2: Data Breach Risk Assessment Factors

Appendix 3: Data Breach Response Plan