Privacy Policy

POLICY OWNER: **Principal**

APPROVED BY: **SLT**

REVIEW DATE: **March 2020**

1.0 PURPOSE

This document outlines the School's policy with respect to how it uses and manages personal information provided to or collected by it.

Hume Anglican Grammar is bound by the 13 *Australian Privacy Principles* contained in the Commonwealth *Privacy Act 1998*. Victorian Government legislation also regulates student and other records. The *Health Records Act 2001 (Vic)* specifically covers health information and applies to the public and private sectors in Victoria.

The School may, from time to time, review and update this Privacy Policy to take account of new laws and technology, changes to the School's operations and practices and to make sure it remains appropriate to the changing school environment.

2.0 SCOPE

This policy and associated procedures applies to all members of the Hume Anglican Grammar community and is inclusive of all school environments (physical and online). It is also applicable to approved visitors, including but not limited to pre-service teachers, guest presenters, volunteers, prospective parents and students.

3.0 ALIGNMENT TO THE STRATEGIC PLAN

Values:

4. RESPECT: principled and disciplined; we care for ourselves and value others
5. INTEGRITY: a community whose members are accountable, responsible and trustworthy
6. SAFETY: care for the health and wellbeing of all members of our community

Goals:	**Pathways:**
3. Staff – professional and dedicated staff committed to the success of the school.	b. establish a supportive and collegial workplace culture based upon optimism, respect and professionalism.
4. Parents – engaging families and forging strong relationships	b. establish a model of home communications based upon the principles of timeliness, openness and trust.

Desired Outcomes:

5. Have staff who are engaged, collegial and dedicated to the School, who find fulfilment in a positive and stimulating workplace.

6. Have connected parents who support the School as an intrinsic and steadfast element of family-life.

4.0 ASSOCIATED DOCUMENTS

Victorian Institute of Teaching - Code of Conduct and Ethics Equal Opportunity Act 2010

Hume Anglican Grammar Information and Communication Technologies policy

Hume Anglican Grammar Staff Laptop policy

Hume Anglican Grammar Parent Volunteer policy

Hume Anglican Grammar Staff Professional expectations policy

Hume Anglican Grammar Child Safety policy and Child Safety Code of Conduct

Hume Anglican Grammar Recruitment and Selection policy

Ministerial Order No. 870 (Child Safe Standards – Managing the Risk of Child Abuse in Schools)

National Catholic Education Commission and Independent Schools Council of Australia Privacy Compliance Manual January 2018

5.0 DEFINITIONS

Personal information: information or an opinion, whether true or not, and whether recorded in a material form or not, about an identified Person, or a Person who is reasonably identifiable. Common examples are a Person's name, signature, address, telephone number, date of birth, medical records, bank account details and commentary or opinion about a Person.

Sensitive information: personal information that is sensitive - information relating to a Person's racial or ethnic origin, political opinions, religion, trade union or other professional or trade association membership, philosophical beliefs, sexual orientation or practices, family court orders or criminal record, that is also personal information; and biometric information about a Person.

Health Information: sensitive information concerning health - includes medical records, disabilities, immunisation details and psychological reports.

Person: is the individual to whom the information applies. In the school context this includes students, parents, staff, contractors and volunteers.

Parent: the legal guardian of the student and signatory of the enrolment contract.

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.

Eligible data breach (EDB): is a Data Breach if it is likely to result in serious harm to an individual or individuals whose information is involved in the Data Breach; therefore, obligating the School to notify any individuals or the Information Commissioner.

6.0 POLICY

6.1 Students and parents

The principal reason the School collects personal information of students and parents, is to enable the School to provide schooling for the student. This includes satisfying the needs of parents, the needs of the student and the needs of the School throughout the whole period the student is enrolled at the School. The purposes for which the School uses personal information of students and parents include:

- to keep parents informed about matters related to their child's schooling, through correspondence, including email, newsletters, the school yearbook and reports;
- day-to-day administration of the School;
- looking after student's educational, social and medical well-being;
- seeking donations and marketing for the School; and
- to satisfy the School's legal obligations and allow the School to discharge its duty of care, for example, in relation to child protection legislation.

In some cases where the School requests personal information about a student or parent and the information requested is not provided, the School may not be able to enrol or continue the enrolment of the student or permit the student to take part in a particular activity.

The type of information the School collects and holds includes (but is not limited to) personal information, including health and other sensitive information, about:

- name, contact details (including next of kin), date of birth, gender, language background, previous school and religion;
- parents' education, occupation and language background;
- medical information (e.g. details of disability and/or allergies, absence notes, medical reports and names of doctors);
- conduct and complaint records, or other behaviour notes, and school reports;
- information about referrals to government welfare agencies;
- counselling reports;
- health fund details and Medicare number;
- any court orders;
- volunteering information; and
- photos and videos at School events.

6.2 Job applicants, Staff members and Contractors

The School's principal reason for collecting personal information of job applicants, staff members and contractors is to assess and (if successful) to engage the applicant, staff member or contractor. The purposes for which the School uses this information include:

- in administering the individual's employment or contract,
- for insurance purposes,
- seeking funds and marketing for the School
- to satisfy the School's legal obligations, for example, in relation to child protection policy.

The type of information the School collects and holds includes (but is not limited to) personal information, including health and other sensitive information, about:

- name, contact details (including next of kin), date of birth, and religion;
- information on job application;
- professional development history;
- salary and payment information, including superannuation details;
- medical information (e.g. details of disability and/or allergies, and medical certificates);
- complaint records and investigation reports;
- leave details;
- photos and videos at School events;
- workplace surveillance information; and
- work emails and private emails (when using work email address) and Internet browsing history.

The School will also collect and retain information on other people who come into contact with the School, including name and contact details and any other information necessary for the particular contact with the School.

6.3 Personal information provided by the Person

The school will generally collect personal information about a Person by means of: forms filled out by Parents or students, face-to-face meetings, interviews, emails and telephone calls. On occasions, people other than Parents and students provide personal information.

6.4 Personal information provided by other parties

In some circumstances the school may be provided with personal information about a Person from a third party, e.g. a report provided by a medical professional or a reference from another school.

6.5 Exception in relation to employee records

Under the *Privacy Act* and *Health Records Act 2001 (Vic)*, the Australian Privacy Principles [and Health Privacy Principles] do not apply to an employee record. As a result, this Privacy Policy does not apply to the School's treatment of an employee record, where the treatment is directly related to a current or former employment relationship between the School and employee.

6.6 School use of personal information

The School's primary purpose is for education and the duty of care of its students. The School will use personal information from a Person for the School's primary purpose and for such other secondary purposes that are reasonably expected, or to which the Person has consented.

6.7 Volunteers

The School also obtains personal information about volunteers who assist the School in its functions or conduct associated activities, such as the Parents and Friends Association, other Parent groups, and alumni associations, to enable the school and the volunteers to work together.

6.8 Marketing and fundraising

The School treats marketing and seeking donations for the future growth and development of the School as an important part of ensuring that the school continues to be a quality learning environment in which both students and staff thrive. Personal information held by the School may be disclosed to an organisation that assists in the School's fundraising, for example, Parents and Friends Association and alumni organisations, other Parents groups or, on occasions, external fundraising organisations.

Parents, staff, contractors and other members of the wider School community may from time to time receive fundraising information. School publications, like newsletters and magazines, which include personal information, may be used for marketing purposes.

6.9 Information Collected by the School

Hume Anglican Grammar collects and holds both personal and sensitive information of students, parents and staff; including but not limited to:

- students and parents before, during and after the course of a student's enrolment at the School;
- job applicants, staff members, volunteers, contractors; and
- other people who come into contact with the School.

6.10 Disclosure of personal information

The School may disclose personal information, not including sensitive information, held about a Person to:

- another school;
- government departments;
- medical practitioners;
- people providing educational, support and health services to the School, including specialist visiting teachers, [sports] coaches, volunteers, and counsellors;
- providers of learning and assessment tools;
- assessment and educational authorities, including the Australian Curriculum, Assessment and Reporting Authority (ACARA) and NAPLAN Test Administration Authorities (who will disclose it to the entity that manages the online platform for NAPLAN);
- people providing administrative and financial services to the School;
- recipients of school publications, such as newsletters and magazines;
- parent or guardians,
- anyone you authorise the School to disclose information to; and
- anyone to whom we are required to disclose the information by law, including child protection laws.

Further, it would be reasonably expected the School to use or disclose personal information in such a way to lessen or prevent a serious threat to the life, health or safety of an individual or to public safety.

6.11 Sending information overseas

A school may disclose personal information about an individual to overseas recipients, for instance, when storing personal information with 'cloud' service providers which are situated outside Australia or to facilitate a school exchange. However, the School will not send personal information about an individual outside Australia without:

- obtaining the consent of the individual (in some cases this consent will be implied); or
- otherwise complying with the Australian Privacy Principles or other applicable privacy legislation.

The School may use online or 'cloud' service providers to store personal information and to provide services to the School that involve the use of personal information, such as services relating to email, instant messaging and education and assessment applications. Some limited personal information may also be provided to these service providers to enable them to authenticate users that access their services. This personal information may be stored in the 'cloud' which means that it may reside on a cloud service provider's servers which may be situated outside Australia.

6.12 Sensitive Information

Sensitive information will be used and disclosed only for the purpose for which it was provided or a directly related secondary purpose, unless the Person agrees otherwise, or the use or disclosure of the sensitive information is allowed by law.

Sensitive information will be used and disclosed only for the purpose for which it was provided or a directly related secondary purpose, unless the Person agrees otherwise, or the use or disclosure of the sensitive information is allowed by law.

6.13 Disclosure of sensitive information

The School may disclose sensitive information, as appropriate, held about a Person to:

- government departments;
- medical practitioners;
- people providing services to the school, including specialist visiting teachers, counsellors and sports coaches;
- anyone you authorise the School to disclose information to; and
- anyone to whom we are required to disclose the information by law.

6.14 Management and security of personal information

The School has in place steps to protect the personal information the School holds from misuse, interference and loss, unauthorised access, modification or disclosure by use of various methods including locked storage of paper records and password access rights to computerised records.

The School stores personal information in a variety of formats including on databases, in hard copy files and on personal devices, including laptop computers.

The security of personal information is of paramount importance and the School takes all reasonable steps to protect the personal information held about Persons from misuse, loss, unauthorised access, modification or disclosure.

These steps include:

- Restricting access to information on databases on a need to know basis with different levels of security being allocated to staff based on their roles and responsibilities and security profile.
- Ensuring all staff are aware that they are not to reveal or share personal passwords.
- Ensuring where sensitive information is stored in hard copy files that these files are stored in lockable filing cabinets in lockable rooms. Access to these records is restricted to staff on a need to know basis.
- Implementing physical security measures at our premises to prevent break-ins.
- Implementing ICT security systems, policies and procedures designed to protect personal information storage on our computer networks.
- Implementing human resources policies and procedures, such as email and internet usage, confidentiality and document security policies, designed to ensure that staff follow correct protocols when handling personal information.
- Undertaking due diligence with respect to third party service providers who may have access to personal information, including a Person's identification providers and cloud service providers, to ensure as far as practicable that they are compliant with the Australian Privacy Principles or a similar privacy regime.

Personal information we hold that is no longer needed, or required to be retained by any other laws, is destroyed in a secure manner, deleted or de-identified as appropriate.

The School website may contain links to other websites. The School does not share personal information with those websites and is not responsible for their privacy practices.

The School's staff are required to respect the confidentiality of students' and Parents' personal information and the privacy of individuals.

See Appendix A for the Confidentiality clause inserted into all employee contracts.

6.15 Access and correction of personal information

Under the Commonwealth *Privacy Act*, a Person has the right to obtain access to any personal information which the School holds about them and to advise the School of any perceived inaccuracy. Students will generally be able to access and update their personal information through their Parents, but older students may seek access and correction themselves.

There are some exceptions to this right, set out in the applicable legislation.

To make a request to access or update any personal information the School holds about a Person, the Principal must be contacted in writing. The School will require the applicant's identity to be verified and the information required specified. Depending upon the nature of the material required, the School may charge a fee to cover the cost of verifying your application and locating, retrieving, reviewing and copying any material requested. If the information sought is extensive, the School will advise the likely cost in advance. If the School cannot provide access to the requested information, it will provide the applicant with written notice explaining the reasons for refusal.

6.16 Consent and rights of access to the personal information of students

The School respects the parent's right to make decisions concerning their child's education.

Generally, the School will refer any requests for consent and notices in relation to the personal information of a student to the student's parents. The School will treat consent given by parents as consent given on behalf of the student, and notice to parents will act as notice given to the student.

As stated in s6.15, parents may seek access to personal information held by the School about them or their child by contacting the Principal. However, there will be occasions when access is denied. Such occasions would include where release of the information would have an unreasonable impact on the privacy of others, or where the release may result in a breach of the school's duty of care to the student.

The School may, at its discretion, on the request of a student grant that student access to information held by the School about them, or allow a student to give or withhold consent to the use of their personal information, independently of their Parents. This would normally be done only when the maturity of the student and/or the student's personal circumstances so warranted.

6.17 Updating personal information

The School endeavours to ensure that the personal information it holds is accurate, complete and up-to-date. A Person may seek to update their personal information held by the School by contacting the School at any time.

6.18 Enquiries and complaints

Further information about the way the School manages the personal information it holds, or for the lodging of complaint, parties are to contact the Principal in writing. The School will investigate any complaint and will notify the individual lodging the complaint of a decision in relation to the matter as soon as is practicable after it has been made.

6.19 Data breaches and eligible data breaches (EDB)

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.

The following are examples of when a Data Breach may occur:

a) loss of smartphone or other School device or equipment containing personal information;
b) cyber-attacks on the School's system, resulting in unknown third parties accessing or stealing personal information;
c) accidental transmission of personal information such as student's reports to unintended recipients via e-mail;
d) loss or theft of hard copy documents; and
e) misuse of personal information of students or parents by School personnel.

Not all Data Breaches will be EDBs. For example, if the 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, the 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.

6.20 Containing a Data Breach

Once the School suspects a Data Breach may have occurred, immediate steps will be taken to identify the Data Breach and if a Data Breach has occurred, to contain and limit it. This may involve stopping the unauthorised disclosure, shutting down the system that was breached, retrieving personal information, or changing computer access privileges or addressing security weaknesses.

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

6.21 Assessing whether the Data Breach is an EDB

The School will determine whether any Data Breach is an EDB. This involves assessing whether:

a) there has been unauthorised access to or unauthorised disclosure of personal information, or a loss of personal information in circumstances where the loss is likely to result in unauthorised access or disclosure; and
b) if so, the Data Breach is likely to result in serious harm to any of the individuals whose personal information was involved; and
c) remedial action is possible.

6.22 Deciding the likelihood of serious harm

Determining whether serious harm is likely is a threshold test and involves considering whether a reasonable person in the School's position would conclude that the Data Breach would be likely (more probable than not) to result in serious harm to any of the individuals to whom the information relates.

This reasonable person test is aimed at ensuring only EDBs are reported to the Information Commissioner – not every Data Breach. EDBs will be Data Breaches:

- that a reasonable person in the School's position (rather than the individual to whom the information relates or any other person) would conclude,
- based on all of the information either immediately available to them, or available following reasonable inquiries or an assessment of the data breach,
- that the unauthorised access to or disclosure of the particular personal information or the particular individual, is likely to result in serious harm to them.

This test is designed to support the objective of the Privacy Act to promote the protection of the privacy of individuals while balancing the interests of entities carrying out their legitimate functions or activities. It also helps avoid unnecessary administrative burdens (both on entities such as Schools, and on the OAIC receiving notification), and 'notification fatigue' on the part of individuals.

6.23 Determining serious harm

Serious harm is not defined in the Privacy Act, however in the context of a Data Breach, the OAIC Resources note that serious harm may include serious physical, psychological, emotional, financial or reputational harm. The Privacy Act contains a non-exhaustive list of 'relevant matters' that may assist the School in assessing the likelihood of serious harm. These include:

i. the kind or kinds of personal information involved;
ii. the sensitivity of that information;
iii. whether the information is protected by one or more security measures and the likelihood any such security measures would be overcome, including the use of an encryption key to circumvent the encryption technology or methodology;
iv. the person, or the kinds of persons, who have obtained, or who could obtain, the information;
v. the likelihood that the person who has obtained the information, or has or could obtain, the information or knowledge required to circumvent the security technology or methodology;
vi. the nature of the harm; and
vii. any other relevant matters.

Each factor is explored in more detail in Appendix D.

6.24 Data Breach response plan

If the School suspects an EDB may have occurred, it will enact the Data Breach response plan as set out in Appendix E.

6.25 Notifying individuals and the Information Commissioner

Once the School is aware that there are reasonable grounds to believe there has been an EDB, the School will, as soon as practicable:

a) make a decision about which individuals to notify;
b) prepare a statement for the Information Commissioner in accordance with the OAIC Notifiable Data Breach (NDB) statement – Form, emailed or lodged online via the OAIC website; and
c) notify individuals of this statement as soon as practicable after notifying the Information Commissioner.

6.26 Voluntary notification

Even when the Data Breach is not an EDB under the notifiable data breaches (NDB) scheme, there may be instances where the School considers it necessary to voluntarily notify one or some affected individuals and the Information Commissioner of a Data Breach, in accordance with its obligations under APP11 to take reasonable steps to keep the personal information it holds secure and complying with its duty of care obligations.

6.27 Reviewing the Data Breach/EDB

Whether the incident that occurs is a Data Breach or an EDB that requires notification under the NDB Scheme, conducting a follow up review of the Data Breach allows the School to prevent future breaches and ensure ongoing compliance with its data security obligations and overarching obligation to manage the personal information it holds in a compliant manner. This includes:

a) investigating and understanding the cause(s) of the Data Breach or EDB;
b) developing a prevention plan and conducting audits to ensure the plan is implemented;
c) considering changes to policies and procedures; and
d) further staff training.

Appendix A - Employee Contract

Confidentiality

An employee, in the course of the employee's employment, will have access to Confidential Information about the School and about its students, parents and employees.

Confidential Information includes information about the affairs, processes, dealings, finances, organisation and personnel, including students, parents and employees, of the School.

Confidential Information may be used solely for the purpose of performing the employee's duties with the School. The employee may only disclose Confidential Information:

- to persons who are aware and agree that the Confidential Information must be kept confidential or to persons who have signed a Confidentiality agreement, as required by the School from time to time, and either:
    - have a need to know (and only to the extent that each has a need to know); or
    - have been approved by the School, as relevant; or
    - that is required by law to be disclosed.

This and similar confidential information is not to be imparted deliberately or carelessly to any person at any time who is not authorised by the Principal to receive it. This obligation continues both during and after the employee's employment with the School.

Where an employee is in possession of documents, software, computers or telecommunication devices containing confidential information or material, the employee is responsible for the security of these items at all times.

A breach of these conditions whilst employed with the School may be grounds for summary termination of employment. If disclosure in breach of these conditions should be made after employment with the School ceases, then the School may apply for an injunction to restrain the breach in addition to claiming damages for losses suffered.

An employee must immediately notify the Principal of any suspected or actual unauthorised use, copying or disclosure of Confidential Information.

The employee must provide assistance reasonably requested by the School in relation to any proceedings that the School may take against any person for unauthorised use, copying or disclosure of Confidential Information.

Annex B - Disclosure statement to students

Counselling at Hume Anglican Grammar – Things You Should Know
The School provides counselling services for its students as part of its approach to student wellbeing. This is provided through the Student Psychologist(s) (the counsellor) employed by the School.

Students are encouraged to make use of this services if they are in need of assistance. There are however a number of things that students and their parents should know before using the counselling service.

1. Records will be made of counselling sessions and because the counsellor is an employee, those records belong to the school, not the counsellor.

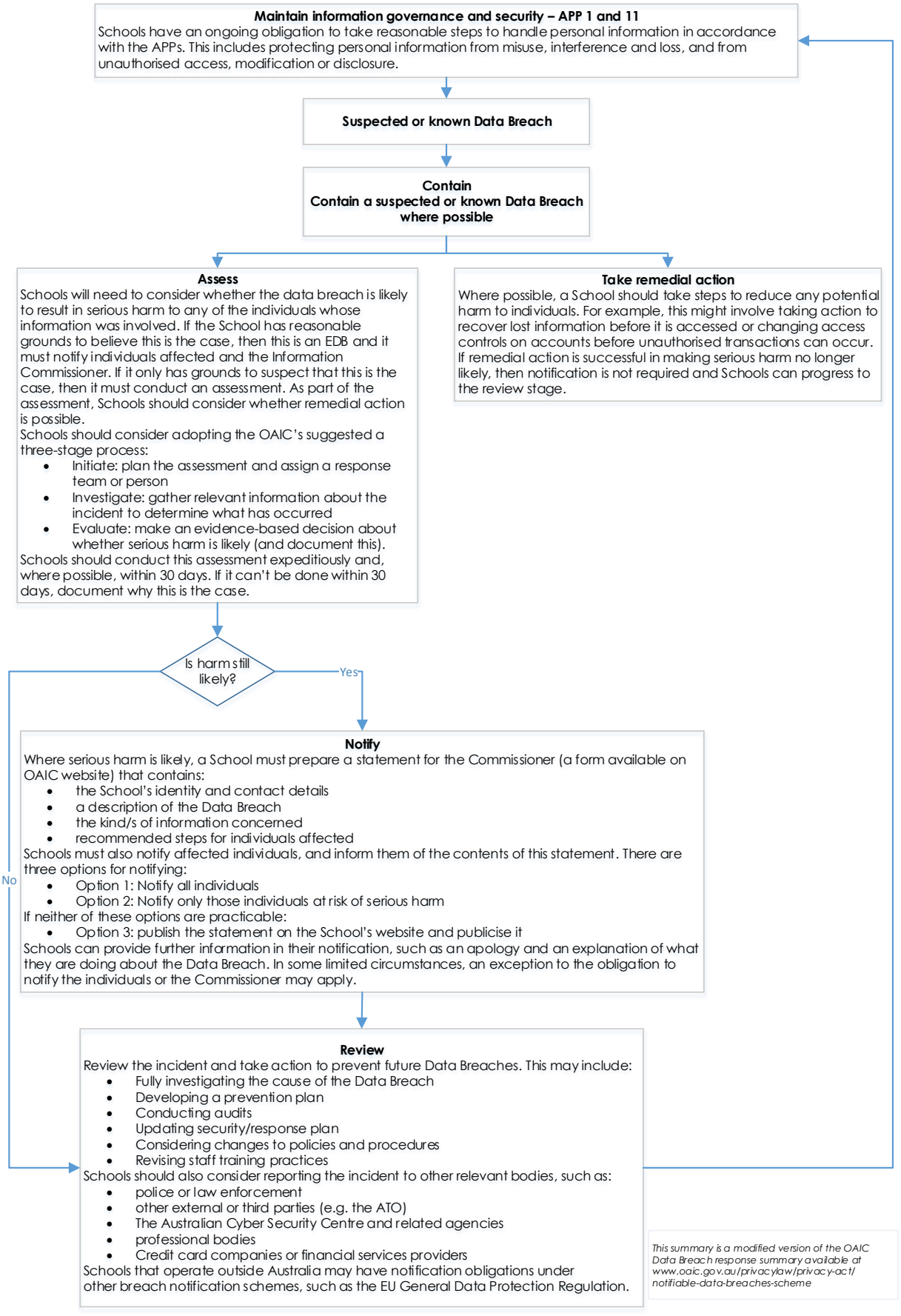
2. The School is very conscious of the need for confidentiality between counsellor and student. However at times it may be necessary for the Counsellor to divulge the contents of discussions or records to the Principal if the Principal or the Counsellor considers it necessary for the student's welfare to discharge the school's duty of care to the student.

3. It is also possible that the Principal may need to disclose aspects of discussions with counsellors to others in order to assist the student.

4. Where a disclosure is made it would be limited to those who need to know, unless the student consents to some wider disclosure.

Hume Anglican Grammar emphasise that disclosures (if any) would be very limited. However if a student is not prepared to use the counselling services on the basis set out above the student will need to obtain counselling services from outside the school.

Annex C - Mandatory notification of eligible Data Breaches summary



Annex D - Data Breach risk assessment factors

Consider who the personal information is about

Who is affected by the breach?
Are students, parents, staff, contractors, service providers, and/or other agencies or organisations affected? For example, a disclosure of a student's personal information is likely to pose a greater risk of harm than a contractor's personal information associated with the contractor's business.

Consider the kind or kinds of personal information involved

Does the type of personal information create a greater risk of harm?
Some information, such as sensitive information (e.g. health records) or permanent information (e.g. date of birth) may pose a greater risk of harm to the affected individual(s) if compromised. A combination of personal information may also pose a greater risk of harm.

Determine the context of the affected information and the breach

What is the context of the personal information involved?
For example, a disclosure of a list of the names of some students who attend the School may not give rise to significant risk. However, the same information about students who have attended the School counsellor or students with disabilities may be more likely to cause harm. The disclosure of names and address of students or parents would also create more significant risks.

Who has gained unauthorised access to the affected information?
Access by or disclosure to a trusted, known party is less likely to cause serious harm than access by or disclosure to an unknown party, a party suspected of being involved in criminal activity or a party who may wish to cause harm to the individual to whom the information relates. For instance, if a teacher at another school gains unauthorised access to a student's name, address and grades without malicious intent (e.g. if the information is accidentally emailed to the teacher), the risk of serious harm to the student may be unlikely.

Have there been other breaches that could have a cumulative effect?
A number of minor, unrelated breaches that might not, by themselves, create a real risk of serious harm, may meet this threshold when the cumulative effect of the breaches is considered. This could involve incremental breaches of the same School database, or known breaches from multiple different sources (e.g. multiple schools or multiple data points within the one school).

How could the personal information be used?
Consider the purposes for which the information could be used. For example, could it be used to commit identity theft, commit financial fraud, abuse the individual either physically or emotionally (including to humiliate the affected individual and social or workplace bullying)? For example, information on students' domestic circumstances may be used to bully or marginalise the student and/or parents. What is the risk of harm to the individual if the compromised information can be easily combined with other compromised or publicly available information?

Establish the cause and extent of the breach

Is there a risk of ongoing breaches or further exposure of the information?
What is the risk of further repeat access, use or disclosure, including via mass media or online?

Is there evidence of intention to steal the personal information?
For example, where a mobile phone has been stolen, can it be determined whether the thief specifically wanted the information on the phone, or the phone itself? Evidence of intentional theft of the personal information (rather than just the device on which it is stored) can suggest an intention to cause harm, which may strengthen the need to notify the affected individual, as well as law enforcement.

Is the personal information adequately encrypted, anonymised or otherwise not easily accessible?
Consider whether the information is rendered unreadable by security measures or whether the information is displayed or stored in way that renders it unusable if breached. If so, the risk of harm to the individual may be lessened.

What was the source of the breach?
For example, was it external or internal? Was it malicious or unintentional? Did it involve malicious behaviour or was it an internal processing error (such as accidentally emailing a student list to an unintended recipient)? Was the information lost or stolen? Where the breach is unintentional or accidental, there is likely to be less risk to the individual than where the breach was intentional or malicious.

Has the personal information been recovered?
For example, has a lost mobile phone been found or returned? If the information has been recovered, is there any evidence that it has been accessed, copied or tampered with?

What steps have already been taken to mitigate the harm?
Has the School fully assessed and contained the breach by, for example, replacing comprised security measures such as passwords? Are further steps required? This may include notification to affected individuals.

Is this a systemic problem or an isolated incident?
When identifying the source of the breach, it is important to note whether similar breaches have occurred in the past. If so, there may be a systemic problem with system security, or there may be more information affected than first thought, potentially heightening the risk.

How many individuals are affected by the breach?
If the breach is a result of a systemic problem, there may be more individuals affected than initially anticipated. The scale of the breach may lead to a greater risk that the information will be misused, so the response must be proportionate. Although it is vital to remember that a breach can be serious despite affecting only a small number of individuals, depending on the information involved.

Assess the risk of harm to the affected individuals.

Who is the information about?
Some individuals are more vulnerable and less able to take steps to protect themselves (e.g. younger students, students with disabilities/special needs, vulnerable families/parents)

What kind or kinds of information is involved?
Some information, such as sensitive information (e.g. health records) or permanent information (e.g. date of birth) or a combination of personal information may pose a greater risk of harm to the affected individual(s) if compromised.

How sensitive is the information?
The sensitivity of the information may arise due to the kind of information involved, or it may arise due to the context of the information involved. For example, a list of the names of some students who attend the School may not be sensitive information. However, the same information about students who have attended the School counsellor or students with disabilities.

Is the information in a form that is intelligible to an ordinary person?
Examples of information that may not be intelligible to an ordinary person, depending on the circumstances may include:

i. encrypted electronic information;
ii. information that the School could likely use to identify an individual, but that other people likely could not (such as a student number that only the School uses – this should be contrasted to a student number that is used on public documents); and
iii. information that has been adequately destroyed and cannot be retrieved to its original form (such as shredded hard copy information).

If the information is not in a form that is intelligible to an ordinary person, what is the likelihood that the information could be converted into such a form?
For example, encrypted information may be compromised if the encryption algorithm is out-of-date or otherwise not fit for purpose and could be broken by a sophisticated attacker, or if the decryption key was also accessed or disclosed in the breach. Even where none of these concerns apply, the School may need to consider the likelihood of the encryption algorithm being broken in the long term.

Is the information protected by one or more security measures?
For example, are the systems on which the information is stored protected by intrusion detection and prevention systems, which identified the attack and stopped the attacker from accessing any information or copying the information?

If the information is protected by one or more security measures, what is the likelihood that any of those security measures could be overcome?
For example, could an attacker have overcome network security measures protecting personal information stored on the network?

What persons (or kind of persons) have obtained or could obtain the information?
Access by or disclosure to a trusted, known party is less likely to cause serious harm than access by or disclosure to an unknown party, a party suspected of being involved in criminal activity or who may wish to cause harm to the individual to whom the information relates. For instance, if a teacher gains unauthorised access to a student's information without malicious intent, the risk of serious harm may be unlikely.

What is the nature of the harm that could result from the breach?
Examples include 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. For example, information on students' domestic circumstances may be used to bully or marginalise the student and/or parents.

In terms of steps to mitigate the harm, what is the nature of those steps, how quickly are they being taken and to what extent are they likely to mitigate the harm?
Examples of steps that may remediate the serious harm to affected individuals might include promptly resetting all user passwords, stopping an unauthorised practice, recovering records subject to unauthorised access or disclosure or loss, shutting down a system that was subject to unauthorised access or disclosure, or remotely erasing the memory of a lost or stolen device. Considerations about how quickly these steps are taken or the extent to which the steps taken are remediating harm will vary depending on the circumstances.

Any other relevant matters?
The nature of other matters that may be relevant will vary depending on the circumstances of the School and the Data Breach.

Assess the risk of other harms.

What other possible harms could result from the breach, including harms to the School?
Examples include loss of public trust in the School, damage to reputation, loss of assets (e.g. stolen laptops), financial exposure (e.g., if bank account details are compromised), regulatory penalties (e.g., for breaches of the Privacy Act), extortion, legal liability, and breach of secrecy provisions in applicable legislation.

Annex E - Data Breach response plan

Introduction

This plan sets out the procedure to manage a School's response to the actual or suspected unauthorised access to or disclosure or loss of personal information (Data Breach). Further guidance about responding to a Data Breach and an eligible data breach (EDB) under the notifiable data breaches scheme (NDB Scheme) is contained in Section 26 of the *Compliance Manual* (January 2018).

Response plan

In the event of a Data Breach, School staff must adhere to the four phase process set out below (as described in the Office of the Australian Information Commissioner's (OAIC) *Notifiable Data Breaches scheme: Resources for agencies and organisations*. It is important that appropriate records and any evidence are kept of the Data Breach and the response. Legal advice should also be sought if necessary.

Phase 1. Confirm, contain and keep records of the Data Breach and do a preliminary assessment

1. The School personnel who becomes aware of the Data Breach or suspects a Data Breach has occurred must immediately notify the Deputy Principal. That person must take any immediately available steps to identify and contain the Data Breach and consider if there are any other steps that can be taken immediately to mitigate or remediate the harm any individual could suffer from the Data Breach.
2. In containing the Data Breach, evidence should be preserved that may be valuable in determining its cause.
3. The Deputy Principal must make a preliminary assessment of the risk level of the Data Breach. The following table sets out examples of the different risk levels.

Risk Level	Description
High	Large sets of personal information or highly sensitive personal information (such as health information) have been leaked externally.
Medium	Loss of some personal information records and the records do not contain sensitive information. Low Risk Data Breach, but there is an indication of a systemic problem in processes or procedures.
Low	A few names and school email addresses accidentally disclosed to trusted third party (e.g. where email accidentally sent to wrong person). Near miss or potential event occurred. No identified loss, misuse or interference of personal information.

4. Where a High Risk incident is identified, the Deputy Principal must consider if any of the affected individuals should be notified immediately where serious harm is likely.
5. The Deputy Principal must escalate High Risk and Medium Risk Data Breaches to the response team (whose details are set out at the end of this protocol).
6. If there could be media or stakeholder attention as a result of the Data Breach, it must be escalated to the response team.

Phase 2. Assess the Data Breach and evaluate the risks associated with the Data Breach including if serious harm is likely

7. The response team is to take any further steps (i.e. those not identified in Phase 1) available to contain the Data Breach and mitigate or remediate harm to affected individuals.

8. The response team is to work to evaluate the risks associated with the Data Breach, including by:
    a. identifying the type of personal information involved in the Data Breach;
    b. identifying the date, time, duration, and location of the Data Breach;
    c. establishing who could have access to the personal information;
    d. establishing the number of individuals affected; and
    e. establishing who the affected, or possibly affected, individuals are.
9. The response team must then assess whether the Data Breach is likely to cause serious harm to any individual whose information is affected by the Data Breach, in which case it should be treated as an eligible data breach (EDB).
10. The response team should also consider whether any of the limited exceptions apply to the Data Breach if it is otherwise an EDB.
11. All reasonable steps must be taken to ensure that the assessment is completed as soon as possible and in any event within 30 days after they suspect there has been a Data Breach.

Phase 3. Consider Data Breach notifications

12. The response team must determine whether to notify relevant stakeholders of the Data Breach, including affected individuals, parents and the OAIC even if it is not strictly an EDB.
13. As soon as the response team knows that an EDB has occurred or is aware that there are reasonable grounds to believe that there has been an EDB, they must prepare a statement with the prescribed information and give a copy of the statement to the Information Commissioner.
14. After completing the statement, unless it is not practicable, the response team must also take such reasonable steps to notify the contents of the statement to affected individuals or those who are at risk from the EDB.
15. If it is not practicable to notify some or all of these individuals, the response team must publish the statement on their website, and take reasonable steps to otherwise publicise the contents of the statement to those individuals.

Phase 4. Take action to prevent future Data Breaches

16. The response team must complete any steps in Phase 2 above that were not completed because of the delay this would have caused in proceeding to Phase 3.
17. The Deputy Principal must enter details of the Data Breach and response taken into a Data Breach log. The Deputy Principal must, every year, review the Data Breach log to identify any reoccurring Data Breaches.
18. The Deputy Principal must conduct a post-breach review to assess the effectiveness of the School's response to the Data Breach and the effectiveness of the Data Breach Response Protocol.
19. The Deputy Principal must, if necessary, make appropriate changes to policies, procedures and staff training practices, including updating this Data Breach Response Protocol.
20. The Deputy Principal must, if appropriate, develop a prevention plan to address any weaknesses in data handling that contributed to the Data Breach and conduct an audit to ensure the plan is implemented.

Response Team

The response team will comprise the permanent members:

- Principal
- Deputy Principal
- Business Manager

Depending upon the nature of the Data Breach or EDB, other staff may include:

- Assistant Principal
- Head of Student Wellbeing
- Representative from Information and Communication Technology Services
- Chaplain
- Student Psychologist

https://www.oaic.gov.au/resources/agencies-and-organisations/guides/app-quick-reference-tool.pdf

Australian Privacy Principles — a summary for APP entities

from 12 March 2014

Australian Government
Office of the
Australian Information Commissioner

APP 1 — Open and transparent management of personal information

Ensures that APP entities manage personal information in an open and transparent way. This includes having a clearly expressed and up to date APP privacy policy.

APP 2 — Anonymity and pseudonymity

Requires APP entities to give individuals the option of not identifying themselves, or of using a pseudonym. Limited exceptions apply.

APP 3 — Collection of solicited personal information

Outlines when an APP entity can collect personal information that is solicited. It applies higher standards to the collection of 'sensitive' information.

APP 4 — Dealing with unsolicited personal information

Outlines how APP entities must deal with unsolicited personal information.

APP 5 — Notification of the collection of personal information

Outlines when and in what circumstances an APP entity that collects personal information must notify an individual of certain matters.

APP 6 — Use or disclosure of personal information

Outlines the circumstances in which an APP entity may use or disclose personal information that it holds.

APP 7 — Direct marketing

An organisation may only use or disclose personal information for direct marketing purposes if certain conditions are met.

APP 8 — Cross-border disclosure of personal information

Outlines the steps an APP entity must take to protect personal information before it is disclosed overseas.

APP 9 — Adoption, use or disclosure of government related identifiers

Outlines the limited circumstances when an organisation may adopt a government related identifier of an individual as its own identifier, or use or disclose a government related identifier of an individual.

APP 10 — Quality of personal information

An APP entity must take reasonable steps to ensure the personal information it collects is accurate, up to date and complete. An entity must also take reasonable steps to ensure the personal information it uses or discloses is accurate, up to date, complete and relevant, having regard to the purpose of the use or disclosure.

APP 11 — Security of personal information

An APP entity must take reasonable steps to protect personal information it holds from misuse, interference and loss, and from unauthorised access, modification or disclosure. An entity has obligations to destroy or de-identify personal information in certain circumstances.

APP 12 — Access to personal information

Outlines an APP entity's obligations when an individual requests to be given access to personal information held about them by the entity. This includes a requirement to provide access unless a specific exception applies.

APP 13 — Correction of personal information

Outlines an APP entity's obligations in relation to correcting the personal information it holds about individuals.

For private sector organisations, Australian Government and Norfolk Island agencies covered by the *Privacy Act 1988*

www.oaic.gov.au