Executive Summary

How Arethusa College handles information collected about individuals (referred to in the Privacy Act 1988 (Cth) (Privacy Act) as personal information) is very important for two main reasons: people we deal with expect us to handle their personal information properly and we have a legal obligation to do so.

There are substantial penalties for serious or repeated breaches of the Privacy Act and the Australian Privacy Principles (APPs). Non-compliance with our privacy obligations also poses a risk of reputational damage to Arethusa College if the privacy of an individual is breached, and further damage if the breach is managed poorly.

Information sharing regimes under state/territory legislation relating to child protection override the privacy requirements under the Privacy Act.

For more information, refer to our Child Protection Program.

About Our Privacy Policy

Under Principle 1 of the Australian Privacy Principles (APPs), Arethusa College is required to develop a Privacy Policy that sets out how we manage personal information and is available on the College's public website.

Our Privacy Policy outlines:

- the types of personal information we collect and hold
- how we collect and hold personal information
- the purposes for which we collect, hold, use and/or disclose personal information
- how an individual can access their personal information and seek a correction of the information

- how an individual may complain about our compliance with the APPs and how we will deal with such a complaint
- whether we are likely to disclose personal information to any overseas recipients, and if so, the countries in which those recipients are based.

Our Privacy Policy is available free of charge.

It is available in the Privacy Documents section of this Program and on our public website.

If a person requests a copy of our Privacy Policy in a particular form, we will take all reasonable steps in the circumstances to provide a copy of the policy in that form.

Privacy Laws and Why They Are Important

Compliance with our privacy obligations is important because the people the College deals with expect us to handle their personal information properly.

Even a minor breach of our legal obligations could cause serious reputational damage to the College. A further failure in our breach management procedures could exacerbate this damage.

People Expect Proper Privacy Protection

Australians are becoming increasingly concerned about privacy risks, particularly how their information is handled in an age of cloud computing and data management.

A survey regarding Community Attitudes to Privacy, conducted by the Office of the Australian Information Commissioner (OAIC) in 2017 found that people are increasingly concerned about information security – 69 per cent of respondents are more concerned about their online privacy than five years ago.

The OAIC found that 58 per cent of respondents had decided not to deal with an organisation because of privacy concerns, up from 40 per cent in 2007, and only 34 per cent trust organisations in general to look after their personal information.

The survey also found that 93 per cent of respondents were concerned about organisations sending their personal information overseas.

The Law Requires Proper Privacy Compliance

Arethusa College is required to comply with the Privacy Act which incorporates the 13 Australian Privacy Principles (APPs). The Privacy Act and the APPs impose substantial privacy on the College meaning that compliance requires more than a privacy policy published on a public website.

The APPs set out the standards, rights and obligations for the College in relation to collecting, storing, using, accessing and correcting personal information.

Breaches of Australian Privacy Principles

The OAIC has significant powers to investigate and penalise organisations for possible breaches of the APPs.

Powers of Investigation

Whether following a complaint, or of its own volition, the OAIC has the discretion to investigate any act, or practice, which may be an interference with privacy, to determine whether a school is handling personal information in accordance with the APPs.

Privacy Assessments

The OAIC also has the power to conduct a privacy assessment of whether a school is complying with the APPs.

Power to Make Orders and Enforceable Undertakings

Where an investigation or privacy assessment has been carried out, the OAIC has the power to:

- make an order that a school pay compensation to an individual whose privacy has been breached; or
- require a school to comply with the terms of an enforceable undertaking that it will refrain from taking, or will take, specified actions to comply with the Privacy Act.

If the College does not comply with an order or enforceable undertaking the order can be enforced through the Federal Court or Federal Magistrates Court.

Power to Seek Penalties

The OAIC can also apply to the Federal Court or Federal Magistrate's Court for significant civil penalties.

What Types of Information are Covered by Privacy Laws?

Privacy is all about how we manage personal and sensitive information (including health information) collected from individuals who deal with our College.

The way we do this is set out in the section How We Handle Personal Information.

The Privacy Act requires the College to handle the personal information (including sensitive information) we collect about individuals in accordance with the 13 Australian Privacy Principles (APPs).

For more information, refer to the following sections:

- Personal Information
- Sensitive Information
- Health Information
- Confidential Information
- Credit Information
- What is a Record?

Personal Information

Personal information is information, or an opinion, about an identified individual, or an individual who is reasonably identifiable:

- whether the information, or opinion, is true or not; and
- whether the information, or opinion, is recorded in a material form or not.

Personal information can be in any format - it is not limited to information that is contained in a record. It can include information that is:

- shared verbally
- captured digitally
- recorded
- captured on signs.

Personal information does not have to contain words. For example, photos or tape recordings can be personal information.

The personal information of one individual can also be personal information of another person or people, known as 'joint personal information'.

Personal information:

- will vary, depending on whether an individual can be identified or is reasonably identifiable in the particular circumstances
- includes information about a person's private or family life such as a person's name, signature, home, address, email address, telephone number, date of birth, medical records, bank account details, financial information, marital status or billing details
- includes information about a person's working habits and practices such as work address and contact details, salary, job title and work practices
- includes an opinion, for example:
    - survey results
    - a referee's comments about a job applicant's career, performance attitudes and aptitude
    - information or opinion inferred about an individual from their activities, such as their tastes and preferences from online purchases they have made from a credit card or from their web browsing history
- can be stored using any medium, for example in a database, email, paper, on disk
- includes sensitive information about individuals.

Personal information does not include:

- information that cannot identify an individual
- information that is not about an individual – because the connection with the individual is too tenuous or remote
- business information. The Privacy Act defines an "individual" as a natural person which does not include a corporate entity (however, if an individual's personal information is so connected to information about their business, it may constitute personal information).
- information about deceased persons (unless that information includes information or an opinion about a living individual)
- information that has been de-identified.

The types of personal information the College collects are noted in our Personal Information Audit, and summarised in our Privacy Policy. A Personal Information Audit Template is available in the Privacy Documents section of this Program.

Sensitive Information

Sensitive information is a subset of personal information relating to individuals, including information or an opinion about their:

- racial or ethnic origin
- political opinions
- membership of a political association
- religious beliefs or affiliations
- philosophical beliefs
- membership of a professional or trade association
- membership of a trade union
- sexual orientation or practices
- criminal record.

Sensitive information about an individual also includes:

- health information
- genetic information that is not otherwise health information
- biometric information and templates.

Sensitive information is generally afforded a higher level of privacy protection and should be treated with additional care. Where practicable, sensitive information should be clearly identified as being such in any records to assist persons handling the information to recognise their sensitive nature. Generally, we require express written consent from a person before we collect and handle their sensitive information.

The types of sensitive information the College collects are noted in our Personal Information Audit, and summarised in our Privacy Policy. A Personal Information Audit Template is available in the Privacy Documents section of this Program.

Health Information

Under the Privacy Act, health information is a subset of sensitive information.

Health information includes any information or opinion collected about:

- the health, including an illness, disability or injury (at any time) of an individual
- an individual's expressed wishes about the future provision of health services to them
- a health service provided, or to be provided, to an individual.

Health information about an individual also includes:

- any personal information collected in relation to a health service the College provides to them
- personal information collected in connection with the donation, or intended donation, by an individual of their body parts, organs or body substances
- genetic information that is, or could be, predictive of the health of the individual or a genetic relative of the individual.

Examples of health information include:

- notes of symptoms or a diagnosis and the treatment given to an individual
- specialist reports and test results
- appointment and billing details
- prescriptions and other pharmaceutical purchases
- dental records
- records held by a fitness club about an individual
- information about an individual's suitability for a job, if it reveals information about the individual's health
- genetic information
- healthcare identifiers
- any other personal information when it is collected for the purpose of providing a health service. For example, information about an individual's date of birth, gender, race, sexuality or religion.

It is the College's policy that health information includes information about an individual's physical, mental or psychological health.

The types of health information the College collects are noted in our Personal Information Audit, and summarised in our Privacy Policy. A Personal Information Audit Template is available in the Privacy Documents section of this Program.

Confidential Information

The term "confidential information" is often used to describe commercially sensitive corporate information, such as financial information of a business or trade secrets. However, the term can also be used to describe information which relates to individuals. For example, a medical practitioner, lawyer, psychologist or counsellor may refer to information about a client as "confidential information".

Confidential information is not a term that is defined within the Privacy Act.

For more information, refer to Confidentiality of Personal Information.

Credit Information

Credit information is defined in the Privacy Act to mean personal information, other than sensitive information, about a person's credit worthiness, credit standing, credit and repayment history or credit capacity that Arethusa College is legally permitted to exchange with credit reporting bodies.

Credit is defined to include a contract, arrangement or understanding under which:

- payment of a debt owed by one person to another is deferred; or
- one person incurs a debt to another person and defers the payment of the debt.

Arethusa College is not a recognised credit provider.

What is a Record?

Personal information is only collected by the College where it is for inclusion in a record or a generally available publication. The College only holds personal information if the College has possession or control of a record that contains the personal information.

The term "holds" extends beyond physical possession of a record to include a record that an entity has the right or power to deal with. For example, if the College outsources the storage of personal information to a third party, but retains the right to deal with the information, including to access and amend it, the College will still "hold" that personal information.

"Record" is a defined term in the Privacy Act and includes a document or an electronic or other device such as a mobile phone.

A record does not include:

- a generally available publication (for example a telephone directory)
- anything kept in a library, art gallery or museum for the purposes of reference, study or exhibition
- letters or other articles in the course of transmission by post.

Whose Information is Protected by the Privacy Act?

The Privacy Act requires us to protect all personal information (including sensitive information and health information) about any individuals who deal with the College.

Who do we collect personal information from?

The College collects personal information from:

- students
- parents/carers and prospective parents/carers
- job applicants
- staff members.

We are also likely to collect personal information from others including:

- alumni
- contractors
- the Board of Directors
- volunteers
- donors
- members of the local community.

Identifying an Individual

The term “individual” is defined in the Privacy Act as any natural person. For example:

- people who are sole traders and people trading in partnerships
- people who represent companies and other organisations, but not including the company or organisation itself
- job applicants up to the point they become College employees. As noted below, the exemption for employees only relates to employee records used directly in the context of the employment relationship.

An individual must be identified or reasonably identifiable for information to constitute personal information.

When is information “about” an individual?

Information is “about” an individual where there is a connection between the information and the individual, and that connection is not too remote. Whether or not information is about an individual is a question of fact, and will depend on the context and circumstances of each case.

When will information be about an "identified" individual?

An individual is "identified" when, within a group of persons, they are distinguished from all other members of the group. There must be a connection between the information and a particular person. The connection does not have to be a name. For example, a photograph or detailed description may also identify an individual.

When is an individual "reasonably identifiable"?

Whether an individual is "reasonably identifiable" from particular information will depend on a number of considerations including:

- The nature and extent of the information. The more information the College holds about an individual, or has access to, the more likely it is that the person will be reasonably identifiable from that information.
- Who will hold and have access to the information. Information that enables an individual to be identified in one context may not identify the individual in a different context. For example, the likelihood of identification will be higher where the subject is known to the person who has access to the information.
- Whether it is possible for us to identify the individual using available resources, taking into account the cost, difficulty, practicality and likelihood of the College doing so. For example, an individual is more likely to be reasonably identifiable from information held by the College when staff have access to, or can easily obtain, other information about the individual. Developments in technology or security may also change the feasibility of a particular method of identifying an individual.

How is information de-identified?

The Privacy Act defines de-identified information as information that is no longer about an identifiable individual, or about an individual who is reasonably identifiable. The process of de-identification involves the removal or alteration of information that identifies a person or is reasonably likely to identify them, as well as the application of any additional protections required to prevent identification. For example, the removal of a name, address or date of birth.

For more information, refer to OAIC Privacy Business Resource 4: De-identification of data and information in the OAIC Guidance Materials section of this Program.

Personal Information of Students

The Privacy Act does not differentiate between adults and children and does not specify an age after which individuals can make their own decisions with respect to their personal information. Although the College will determine on a case-by-case basis whether a student under the age of 18 has the capacity to consent and make decisions in respect of student information, generally we will refer any requests for personal information to a student's parents/carers. We will treat notices provided to parents/carers as notices provided to a student and we will treat consents provided by parents/carers as consents provided by a student.

The College recognises that children have rights under the Privacy Act and that, in certain circumstances (especially when dealing with older students or when dealing with sensitive information), it will be appropriate to seek and obtain consent directly from students. How the College collects, manages, uses and discloses student information will be dealt with on a case-by-case basis.

The Employee Records Exemption

Acts or practices relating to employee records of an individual are exempt from the Privacy Act, if the acts or practices directly relate to a current or former employment relationship between the employer and the individual.

An "employee record" is a defined term in the Privacy Act and means a record of personal information relating to the employment of the employee. Examples of employee records include:

- health information
- the engagement, training, disciplining, resignation or termination of employment of an employee
- terms and conditions of employment
- personal and emergency contact details, performance or conduct, hours of employment or salary or wages
- membership of a professional or trade organisation or trade union membership
- recreation, long service, sick, maternity, paternity or other leave
- taxation, banking or superannuation affairs information.

Not all information that relates to an individual employee will be considered an employee record. For example, emails received via an employee's work email account may not necessarily be part of an employee record as they may not relate to the employment of the employee.

This exemption excludes:

- employees that are employed through a related corporation

- employee records that are provided to a third party such as an industry association or educational authority
- future employment relationships, i.e. personal information collected from prospective employees who are subsequently not employed by the College, such as unsuccessful job applicants
- volunteers
- contractors and sub-contractors.

Even though employee records are exempt from the Privacy Act, it is important that individual employee records are maintained securely and information about these records only be disclosed on a strict need-to-know basis.

It is the College's policy that employee-related information is only collected when we believe is necessary for the management of the employment relationship and that employee information is securely maintained and only disclosed on a need-to-know basis.

The practical effect of the employee records exemption is that employees are unable to use the provisions of the Privacy Act to access their personal information.

Health Information

Information relating to employees' medical conditions, and in particular to work-related injury or illness, is likely to be further protected by employment, work health and safety and worker's compensation laws.

The HR Act will apply to employees' health information.

Disclosure to Other Entities

The employee records exemption will only apply to personal information held by the College. If employee personal information is disclosed to another entity, the Privacy Act will govern the handling of that information by the entity, unless it is exempt from the application of the Privacy Act.

For more information, refer to Transfers Between Related Bodies Corporate.

Our Privacy Officer

Arethusa College's Executive Principal, Lisa Coles is our Privacy Officer.

Our Privacy Officer can be contacted at:

- lisa.coles@arethusa.qld.edu.au
- 1300 720 371

Responsibilities of our Privacy Officer

Our Privacy Officer is the first point of contact for advice on privacy matters related to the College. The Privacy Officer is responsible for:

- promoting a culture where the personal information of individuals is protected in accordance with our obligations under the Privacy Act
- integrating privacy obligations into existing practices and procedures and policy documents
- providing or organising ongoing training support for managers to ensure that all relevant persons receive privacy training
- managing privacy queries and complaints
- in association with a Data Breach Response Team, managing and assessing, and coordinating responses to, data breaches
- liaising with regulators (where necessary)
- monitoring privacy compliance performance
- analysing performance to identify the need for corrective action
- ensuring privacy issues are factored into contracts with external suppliers
- ensuring our Privacy Program and Privacy Policy are reviewed on a regular basis
- ensuring Personal Information Audits are conducted on a regular basis to determine how the College collects, uses and discloses personal information.

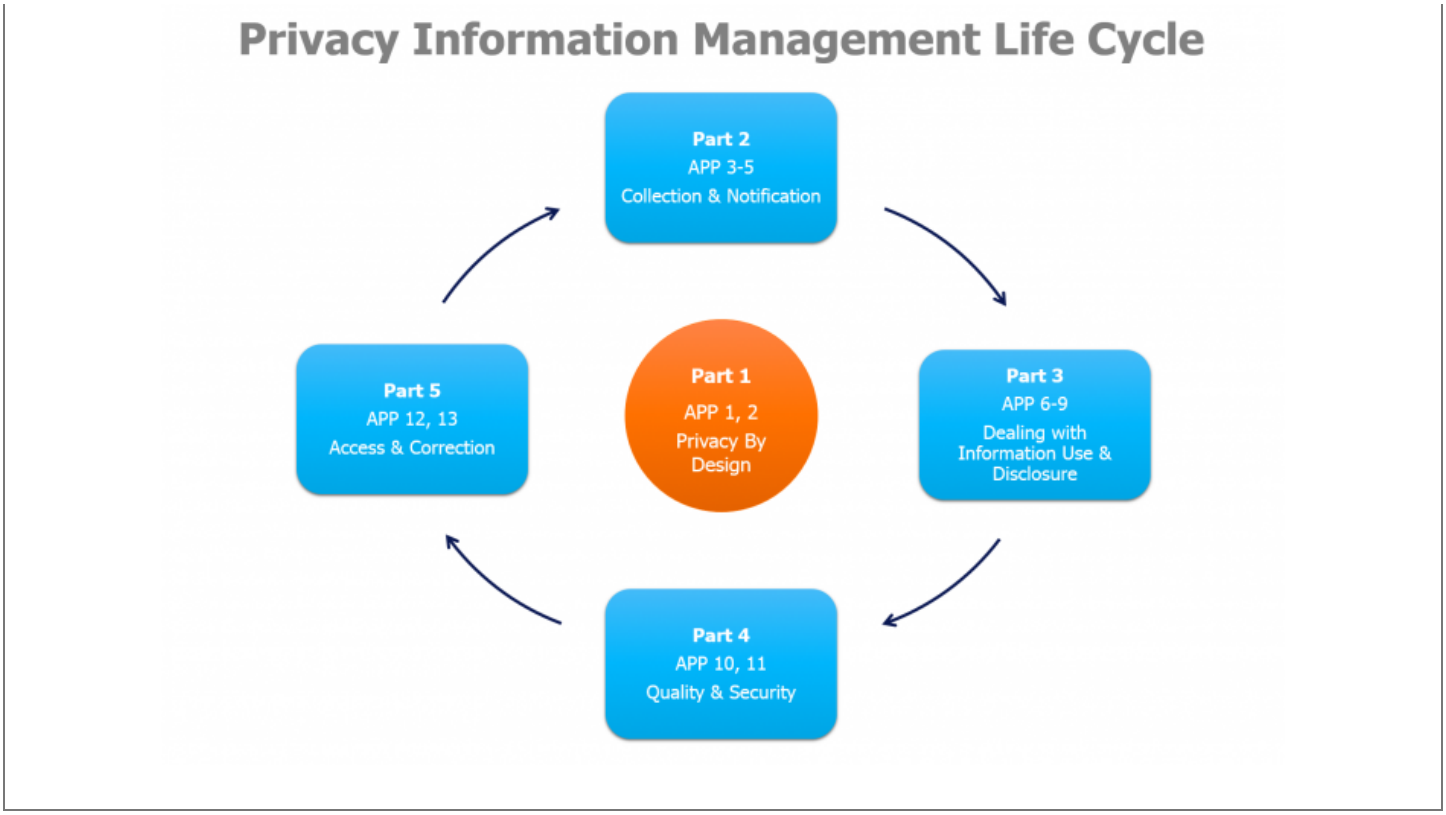
Our Privacy Officer will be responsible for notifying the OAIC in the event of a data breach. For more information, refer to our Procedures for Responding to and Reporting Data Breaches.

The 13 Australian Privacy Principles - How We Handle Personal Information

The 13 Australian Privacy Principles (APPs) set out how we handle the personal information we collect and use about individuals.

The APPs can be categorised into five parts.

These five parts follow a Privacy Information Management Life Cycle as illustrated in the following diagram:



Part 1 – Privacy by Design

Principle 1: Open and Transparent Management of Personal Information

Principle 2: Anonymity and Pseudonymity

Part 2 – Collection and Notification

Principle 3: Collection of Solicited Personal Information

Principle 4: Dealing with Unsolicited Personal Information

Principle 5: Notification of the Collection of Personal Information

Part 3 - Dealing with Information Use and Disclosure

Principle 6: Use or Disclosure of Personal Information

Principle 7: Direct Marketing

Principle 8: Cross-Border Disclosure of Personal Information

Principle 9: Adoption, Use or Disclosure of Government-Related Identifiers

Principle 1: Open and Transparent Management of Personal Information

The Legal Requirement

The College must establish and effectively implement practices, procedures and systems that ensure:

- we comply with each of the APPs; and
- we are able to deal with inquiries or complaints from individuals about our compliance.

The objective of this Principle is to ensure that we manage personal information in an open and transparent way.

How We Comply with This Obligation

Arethusa College is committed to managing personal information in an open and transparent way, and to this end we have adopted the “privacy by design” approach required under Principle 1, which allows us to effectively manage personal information in accordance with the APPs.

Our Internal Practices, Procedures and Systems

We have implemented the following internal practices, procedures and systems:

- the establishment of this Privacy Program which sets out how we comply with each of the APPs set out in the Privacy Act
- the publication of our Privacy Policy through which we disclose how we manage personal information on a day-to-day basis
- undertaking regular Personal Information Audits to review the types of personal information we collect, how we disclose it, how and where we store it and the security procedures that we have

implemented to protect this information (a Personal Information Audit Template is available in the Privacy Documents section)
- the development of privacy consent forms that give the individual the opportunity to choose which collections, uses and disclosures they consent to. Note: We do not use the practice of “bundled consents” as they have the potential to undermine the voluntary nature of consent
- the development of a Data Breach Response Plan that gives staff documented procedures to follow to manage a Data Breach incident and make any required notifications
- the establishment of a Risk Management Program that substantially meets the guidelines as set out in the International Risk Management Standard AS/NZS ISO 31000:2009, through which we manage privacy related risks
- the establishment of a Compliance Program which meets the guidelines as set out in the International Compliance Standard ISO 19600:2014. Our Compliance Program is designed to ensure legal and regulatory, organisational and contractual compliance including compliance with the APPs
- the establishment of a Complaints Handling Program that was designed in line with the Australian Complaints Handling Standard (AS/NZS 10002:2014) and the International Complaints Handling Standard (ISO 10002:2014), through which we manage privacy-related complaints
- the implementation of CompliSpace Assurance, a workflow management database, that allows us to capture risks and compliance tasks and as well as incidents (such as privacy inquiries and complaints), assign them to responsible individuals, monitor individual performance and report in real time
- the development of a Privacy Training Program to ensure key aspects of our Privacy Program are effectively communicated to staff
- the development of associated policies and procedures designed to ensure compliance with the privacy laws which are integrated into our day-to-day operations
- regular reporting to the Management Team and Board on risk and compliance issues (including privacy)
- the formal endorsement of our Privacy Program by our Board
- regular review of our Privacy Program and our Privacy Policy (as well as associated policies) to ensure that they remain relevant and continue to ensure our ongoing compliance with privacy laws.

Our Privacy Policy

Under Principle 1, Arethusa College is required to develop a Privacy Policy that sets out how we manage personal information and is available on the College's public website.

Our Privacy Policy outlines:

- the types of personal information we collect and hold
- how we collect and hold personal information
- the purposes for which we collect, hold, use and/or disclose personal information
- how an individual can access their personal information and seek a correction of the information
- how an individual may complain about our compliance with the APPs and how we will deal with such a complaint
- whether we are likely to disclose personal information to any overseas recipients, and if so, the countries in which those recipients are based.

Our Privacy Policy is available free of charge.

It is available in the Privacy Documents section of this Program and on our public website.

If a person requests a copy of our Privacy Policy in a particular form, we will take all reasonable steps in the circumstances to provide a copy of the Policy in that form.

Principle 2: Anonymity and Pseudonymity

The Legal Requirement

The College is required to give individuals who deal with Arethusa College the option of not identifying themselves or the option of using a pseudonym unless:

- the College is required by law to deal with individuals who have identified themselves; or
- it is impracticable for us to deal with an individual who does not identify themself or has used a pseudonym.

Anonymity means that an individual cannot be identified and the College cannot collect personal information or identifiers. It also means the College cannot identify the individual after the collection of the information. An example of an anonymous dealing is an unidentified individual telephoning the College to inquire generally about our services.

A pseudonym is a name, term or descriptor that is different to an individual's legal name. An example is an email address that does not contain the person's legal name.

How We Comply with This Obligation

Individuals dealing with the College have the option of doing so anonymously or by using a pseudonym.

The effect of an individual opting to deal with us in this way is that the individual's personal information or identifiers cannot be collected, thereby allowing the individual to exercise greater control over their personal information.

We are required to make all individuals aware of this option, and do so through our Privacy Policy.

In some cases, an individual using a pseudonym may choose to divulge their identity or volunteer personal information necessary to complete a particular transaction, such as credit information. In this case, the personal information should only be linked to the pseudonym if:

- it is required or authorised by law
- it is impracticable for the College to act differently
- the individual has consented to providing or linking the personal information.

In circumstances where it is impracticable for the College to deal with individuals who have not identified themselves (for example a complaint may not be able to be investigated and resolved without identifying the complainant) or where we are required by law or court order to deal with identified individuals only, then individuals will not have the option of retaining anonymity or using a pseudonym.

Principle 3: Collection of Solicited Personal Information

The APPs differentiate between "solicited information" and "unsolicited information".

Solicited information is the information the College has asked an individual to provide.

Unsolicited information is information that has been provided to the College, by an individual, without the College requesting the information. Unsolicited information is dealt with under Principle 4: Dealing with Unsolicited Personal Information.

The Legal Requirement

The College must not collect solicited personal information (including sensitive information) unless the information is reasonably necessary for one or more of our functions or activities*.

Generally, the College must not collect sensitive information unless the individual has consented, it is required by law (including meeting our student duty of care obligations), or - if it is impractical to

obtain the individual's consent - the information is necessary to prevent or lessen a serious threat to the life or health of an individual.

We must only collect personal information by lawful and fair means and not in a way that can be interpreted as unreasonably intrusive.

Unless we have obtained an individual's consent, the College must only collect personal information directly from them, unless it is unreasonable or impractical to do so.

*The College's functions and activities include current and proposed functions and activities and those activities we carry out in support of our other functions and activities, such as human resources and corporate administration.

How We Comply with This Obligation

Personal Information We Actively Collect

The College "collects" information if it is for the purpose of including the information in a record or generally available publication (magazine, article, newsletter etc.) (refer to What is a Record?).

Arethusa College only actively collects personal information (including sensitive information) that is reasonably necessary for one or more of the College's functions or activities.

Whether collection is reasonably necessary requires an objective assessment of factors associated with the collection for the function or activity. For example, considering whether we could undertake the function or activity without collecting the personal information, or by collecting a lesser amount of personal information.

If the personal information is sensitive information (including health information), then the College will obtain the individual's consent (which may be implied) to the collection, unless:

- the collection of the sensitive information is required or authorised by law
- it is unreasonable or impractical to obtain the individual's consent and the collection is necessary to prevent or lessen a serious threat to the life or health of any individual
- other specific circumstances exist for sensitive information which is health information.

Refer to the OAIC Guidance Materials section for more information about Permitted General Situations and Permitted Health Situations.

For details of the types of personal, sensitive and health information the College collects refer to What Types of Information are Covered by Privacy Laws.

How We Collect Personal Information

The College may collect personal information any time we deal with an individual.

We are committed to ensuring that collection only occurs by lawful and fair means including:

- by phone
- by email
- by mail
- using a form
- through our public website
- over the counter
- in face-to-face meetings with an individual
- through surveillance such as CCTV or monitoring of computer networks
- through the use of “cookies” for web browsing.

Care must be taken when collecting sensitive information to not do so in the presence of others, and not to advise an individual that it is compulsory to provide information when it is not. These actions may be considered unfair or unreasonably intrusive. Other examples of when it is inappropriate to collect sensitive information include if a person is traumatised, in a state of shock or intoxicated or if we misrepresent the effect of collection.

Collection through Surveillance

Where we have implemented surveillance systems such as cameras, or systems for monitoring computer networks, we must take all reasonable steps to inform people that they may be being monitored and that personal information may be collected. The information will be personal information where a person is identifiable, or reasonably identifiable from the footage.

Arethusa College has developed a number of policies that deal with the collection of personal information through surveillance that can be found in our Work Health and Safety, Human Resources and Student Duty of Care policies and procedures.

Collection of Information Directly from the Individual

The Privacy Act requires that personal information must be collected directly from an individual unless it is unreasonable or impractical for us to do so.

Whether it is unreasonable or impractical to collect personal information directly from an individual will depend on a range of considerations including:

- the difficulty of collecting the information from the individual
- whether the individual would reasonably expect the information to be collected from them or from another source
- the sensitivity of the information
- whether direct collection would jeopardise the integrity of the information or the purpose of collecting it
- whether the cost of collecting the information directly would be excessive
- privacy risks if the information is collected from another source.

At Arethusa College, it is often impractical to collect information directly from an individual. Examples of such situations include:

- a student's personal information may be collected from a variety of third party sources including from their parents/carers, health professionals, teachers, government agencies, other schools and related associations
- a parent's/carer's/relative's personal information may be collected from a student, a relative, a fundraising body, another parent/carer, health professionals, teachers and government agencies
- a staff member's or prospective staff member's personal information may be collected through other schools, referees, school associations and government agencies
- personal information of others, including siblings, referees, next of kin, emergency contacts, spouses, previous employers etc. may be collected indirectly as others complete forms and provide information to the College.

In most scenarios, the individual concerned will be aware of this indirect collection and consent can be inferred, however this will not always be the case, and where personal information is obtained from a third party (particularly sensitive information) without the individual's knowledge, the College should inform the individual that they have collected the information.

Collection of Information Directly from a Related Body Corporate

We may collect personal information (other than sensitive information) directly from a related body corporate without meeting the "reasonably necessary" requirements. For more information, refer to Transfers Between Related Bodies Corporate.

Principle 4: Dealing with Unsolicited Personal Information

The College may receive personal information about an individual in circumstances where we have taken no active step to collect the information. This is known as unsolicited personal information.

Examples of unsolicited personal information the College collects include:

- a note from a student or their parents/carers
- misdirected mail
- petitions including names and addresses
- job applications not in response to an advertised job vacancy
- a promotional flyer/leaflet promoting an individual's business containing an email address or mobile phone number
- personal information that is provided to us that is additional to the information solicited by us (for example if an individual completes an application or information request and provides additional personal information that was not requested).

The Legal Requirement

If the College receives unsolicited information, we must determine whether it is necessary for one or more of our activities or functions.

If it not necessary, we must destroy or de-identify it.

If it is necessary, we must treat it as we would treat any solicited information we have collected.

How We Comply with This Obligation

If unsolicited personal information received by the College could not have been collected under Principle 3: Collection of Solicited Personal Information, we will destroy or de-identify the information as soon as practicable, provided it is lawful and reasonable to do so. The College will consider technical and resource considerations when determining a timetable that is practicable.

It should be noted that collection of personal information only occurs where a record is made of the information (refer to What is a Record?).

Given that on many occasions it is likely that unsolicited personal information will be received orally, it is important for all staff to understand that this information will only be caught by the privacy laws in the event it is subsequently recorded.

Principle 5: Notification of the Collection of Personal Information

The Legal Requirement

At or before the time of collection (or if not practical, as soon as practical afterwards), the College must take reasonable steps to notify an individual about, or ensure an individual is aware of, certain matters concerning the purpose and circumstances of the collection of their personal information.

This requirement applies to solicited and unsolicited personal information (that is not de-identified or destroyed – refer to Principle 4: Dealing with Unsolicited Personal Information).

Information which we are required to provide to individuals includes:

- our College's identity and contact details
- the fact and circumstances of collection if the individual may be unaware that the information has been collected or of the circumstances of collection
- details of the relevant law where the collection of the personal information is required or authorised by law
- the purposes of collection (including secondary purpose if relevant)
- the consequences if the personal information is not collected (for example the individual's complaint may not be able to be properly investigated or resolved)
- details of any other entities or types of entities to whom the collected information may usually be disclosed (for example, contact details, employment history). Such entities should be named if practical to do so.
- whether our organisation will disclose personal information to overseas recipients, and if practical, the countries in which those recipients are located
- information about our Privacy Policy which includes information on how to make a privacy complaint and how an individual can access and seek correction of their personal information.

It is important to note that the College is only required to take "reasonable steps" to inform people of such matters (noted above) that are "reasonable in the circumstances".

Deciding what is reasonable involves balancing the sensitivity of the information to the individual and the time and cost to the College in providing that information. It would not be expected that we provide notification of matters that are considered to be obvious or likely to be known.

Factors which may support a decision that notification would be unreasonable include if the notification would be inconsistent with another legal obligation (such as legal professional privilege or obligation of confidence) and impracticability (time and cost).

How We Comply with This Obligation

We comply with our obligations with respect to the notification of collection of personal information through a combination of:

- our Privacy Policy
- the use of Standardised Information Collection Forms which incorporate a Privacy Collection Notice.

Our Privacy Policy

Our Privacy Policy sets out how we manage personal information including:

- who we collect information from
- the types of personal information we collect and hold
- how we collect and hold personal information
- the purposes for which we collect, hold, use and/or disclose personal information
- how an individual can access their personal information and seek a correction of the information
- how an individual may complain about our compliance with the APPs and how we will deal with such a complaint
- whether we are likely to disclose personal information to any overseas recipients, and if so, the countries in which those recipients are based.

A copy of our Privacy Policy is published on our public website and made available on request.

Standardised Information Collection Forms

Where possible, the College has attempted to standardise the collection of personal information by using specifically designed forms (e.g. an Enrolment Form, a Health Information Form), which include a Privacy Collection Notice.

Principle 6: Use or Disclosure of Personal Information

The Legal Requirement

Use or Disclosure for a Primary Purpose

The College must only use or disclose personal information it holds for the primary purpose for which it was collected. The terms “use” and “disclose” are not defined in the Privacy Act and the below definitions are taken from OAIC Guidance.

“Use” of personal information occurs where the College handles or undertakes an activity with the information. This includes acts such as:

- accessing and reading the information
- searching records that contain the information
- making a decision based on the information
- transferring the information from one part of our organisation to another part or a related body corporate
- unauthorised access by a College employee.

“Disclosure” of personal information occurs where the College makes the information accessible to others outside Arethusa College. This includes any act that permits the information to become known outside of the College and releases it from our effective control. The release may be a proactive release or publication, a release in response to a specific request, an accidental release or an unauthorised release by an employee. Examples include sharing the personal information with another entity or individual, publishing the information on the internet (whether intentionally or not) and revealing the personal information in the course of a conversation with a person outside of the College.

Disclosure is a separate concept from unauthorised access (Principle 11: Security of Personal Information).

“Primary Purpose” is not a defined term, however the context of the collection of the information will more often than not identify the primary purpose. Most personal information collected by a school will be for the primary purpose of providing educational services including complying with its common law duty of care obligations. The precise purpose, however, will depend on the circumstances.

Use or Disclosure for a Secondary Purpose

The College may only use or disclose personal information for a secondary purpose (i.e. any purpose other than the primary purpose) if one or more of the following circumstances exist:

- the individual has consented to a secondary use or disclosure
- the individual would reasonably expect the use or disclosure of the personal information for the secondary purpose and the secondary purpose is related to the primary purpose of collection. In line with the individual’s reasonable expectations, we will only use or disclose the personal information, or part thereof, to the extent necessary for the secondary purpose

- in the case of sensitive information, the individual would reasonably expect the use or disclosure of the sensitive information for the secondary purpose and the secondary purpose is directly related to the primary purpose (i.e. it is closely associated with the primary purpose, even if it is not necessary to achieve the primary purpose)
- a Permitted General Situation such as the following exists in relation to the use or disclosure:
    - where the College reasonably believes that the use or disclosure is necessary to lessen or prevent a serious threat to the life, health or safety of an individual or to public health or safety
    - where the College has reason to suspect that unlawful activity or misconduct of a serious nature is being or has been engaged in
    - where the College believes that the use or disclosure is necessary to assist in locating a missing person
    - where the use or disclosure is reasonably necessary to establish, exercise or defend a legal claim
    - where it is reasonably necessary for confidential alternative dispute resolution processes
    - where it is necessary for a diplomatic or consular activity or for certain Defence Force activities outside Australia
- a Permitted Health Situation such as the following exists in relation to the use or disclosure:
    - the use or disclosure of health information of an individual for research relevant to public health or safety and it was impracticable to obtain the consent of the individual
    - in relation to genetic information obtained in the course of providing a health service, where we believe that the use or disclosure is necessary to lessen or prevent a serious threat to life, health or safety of a genetic relative of the individual
    - the use or disclosure of health information to a responsible person for the individual (e.g. a carer providing a health service) is necessary to provide appropriate care or treatment or for compassionate reasons
- it is authorised by law or a court/tribunal order
- it is reasonably necessary for one or more law enforcement related activities.

How We Comply with This Obligation

The College complies with our obligations with respect to use and disclosure of personal information through:

- our Privacy Policy
- the use of Standardised Information Collection Forms that incorporate a Privacy Collection Notice

- the use of specific consent requests.

Our Privacy Policy

Our Privacy Policy sets out how we manage personal information including:

- the types of personal information we collect and hold
- how we collect and hold personal information
- the purposes for which we collect, hold, use and/or disclose personal information
- how an individual can access their personal information and seek a correction of the information
- how an individual may complain about our compliance with the APPs and how we will deal with such a complaint
- whether we are likely to disclose personal information to any overseas recipients, and if so, the countries in which those recipients are based.

In our Privacy Policy, we clearly set out the secondary purposes for which personal information may be used to assist us in establishing an individual's "reasonable expectations" as to the use of their personal information.

We have developed a Guide to Use or Disclosure of Personal Information which is designed to assist our staff in making decisions with respect to the use and disclosure of personal information within the College.

A PDF of the Guide is available in the Privacy Documents section of this Program.

Standardised Information Collection Forms

Where possible, the College has attempted to standardise the collection of personal information by using specifically designed forms (for example an Enrolment Form, a Health Information Form), including a Privacy Collection Notice.

Consent Requests

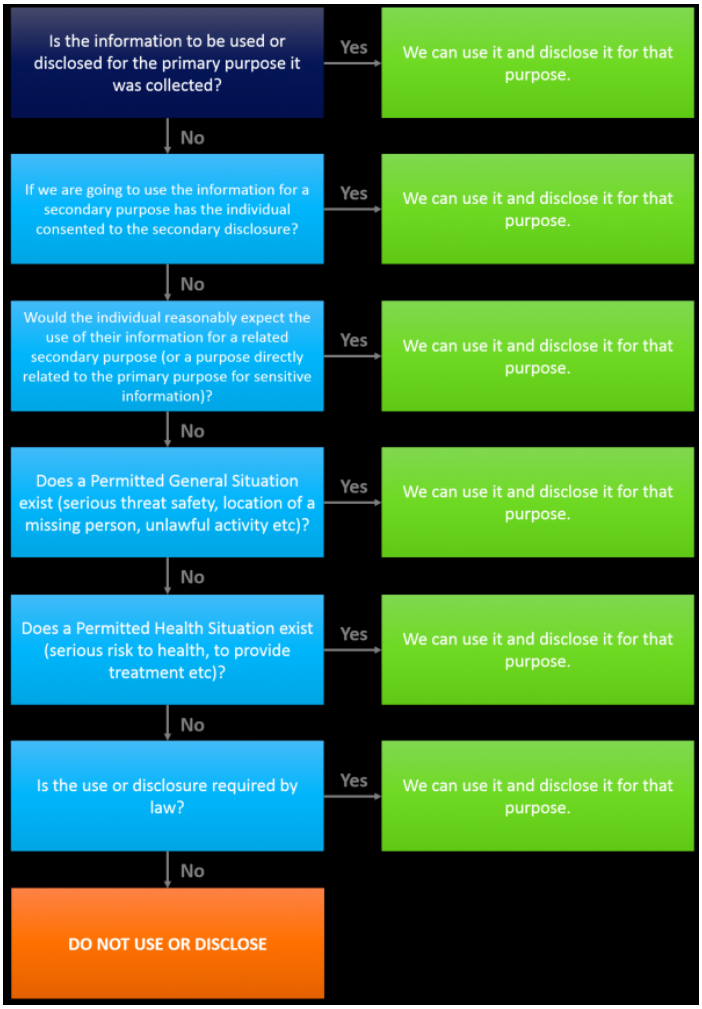
In certain circumstances such as when we seek:

- to use personal information (other than sensitive information) for a secondary purpose, where an individual may not reasonably expect us to use information in this way (e.g. the distribution of a parent's contact details to other parents or use of a child's photograph in our College's promotional material); or

- to use sensitive information for a purpose which is not directly related to the primary purpose for which we collected it,

we will seek specific written consent for the collection and use of the information for this purpose.

Guide to Use or Disclosure of Personal Information



Principle 7: Direct Marketing

The Legal Requirement

Direct marketing involves the use or disclosure of personal information to communicate directly with an individual to promote goods or services through a channel such as telephone, SMS, mail, email and online advertising.

The College must not use or disclose personal information for the purpose of direct marketing, unless one of the following situations exists:

- where we have collected personal information directly from the individual, and they would reasonably expect us to use or disclose the information for direct marketing, we provide a simple means for the individual to request not to receive direct marketing communications from us and they have not done so.
- where we have collected personal information either directly from the individual, or from a third party, and the individual would not have a reasonable expectation that we would use it for direct marketing, we either:
    - obtain the individual's consent
    - if obtaining consent is impractical, in each direct marketing communication, we include a prominent statement that the individual may request not to receive direct marketing communications from us, and the individual has not made such a request.
- if the information is sensitive information, including health information, the individual has consented to its use. Consent can be express or implied.

How We Comply with This Obligation

It is the College's policy that:

- we do not use sensitive information for direct marketing purposes unless we have the individual's consent to do so
- if we use an individual's personal information for the purpose of direct marketing (for example fundraising), in each direct marketing communication we include a prominent statement allowing the individual to request not to receive direct marketing material. This is also known as "opting out".
- in the event that we receive an opt out request we comply with this request and update our databases accordingly.

Principle 8: Cross-Border Disclosure of Personal Information

Our Legal Liability

Where the College discloses personal information to an overseas recipient, the College is legally accountable if the overseas recipient mishandles the personal information, unless one of the following applies:

- the overseas recipient is subject to the laws of a country, or a binding scheme, that we reasonably believe to be substantially similar to the protections afforded to personal information under the APPs and an individual can access mechanisms to enforce the protections of the law or binding scheme
- we have the individual's consent, after expressly informing them in a statement of the potential consequences of providing consent
- a Permitted General Situation or a Permitted Health Situation exists (refer to OAIC Guidance Materials section for more information).

When would it be likely to disclose information to an overseas recipient?

Examples of when we may disclose personal information to an overseas recipient include:

- publishing unsecured personal information using a cloud-based computer storage service with servers based outside Australia
- sending emails or hard copy documents containing personal information to an overseas recipient, especially when organising overseas trips or facilitating a student exchange
- discussing personal information at an overseas meeting or with an overseas recipient over the phone and making a record of it
- publishing personal information on the internet (for example on social media sites such as Facebook or Twitter) that is accessible by overseas recipients
- using online applications (apps or other services) provided by an overseas third party service provider for services such as email, instant messaging, learning and assessment tools
- providing personal information to an overseas contractor or service provider including for excursions.

Minimising Our Risks in Relation to Cross-Border Disclosure of Personal Information

The College minimises our risks in relation to cross-border disclosure of personal information by:

- regularly reviewing our information storage and distribution practices, processes and systems, to identify scenarios where personal information may potentially be disclosed to an overseas recipient
- maintaining a register of all Cloud Based Service Providers the College uses, identifying where our data is being stored, and in the event it is being stored overseas, satisfying ourselves that appropriate arrangements are in place to limit our exposure should a data breach occur.
- ensuring that any Cloud Based Service Providers, whose services are provided using overseas data-centres, are required to provide undertakings with respect to protection of personal

information and to provide an indemnity to protect the College in the event we are subject to a claim as a result of a data breach
- including information in our general Privacy Policy with respect to cross-border disclosure in the event that any personal information we collect may be disclosed to an overseas recipient. This general disclosure is designed to cover issues such as organising overseas excursions and facilitating student exchanges
- ensuring that no personal information is published by the College via social media platforms, unless an individual's consent to the disclosure has been expressly sought and obtained
- ensuring that no personal information is published on publicly accessible internet sites (including the College's public website) unless an individual's consent to the disclosure has been expressly sought and obtained
- seeking specific consent prior to disclosure whenever the College needs to disclose personal information overseas for a particular purpose, such as for an overseas excursion or exchange.

Note: The APP Guidelines provide that where personal information is routed through servers located outside Australia, this will generally be considered a use and not a disclosure. This is because the entity does not release the subsequent handling of personal information from its effective control. Compliance with Principle 8 is not required in this case.

Principle 9: Adoption, Use or Disclosure of Government-Related Identifiers

The Legal Requirement

The College must not use government-related identifiers (for example Medicare numbers, Tax File Numbers, Centrelink identifiers or drivers' licences) as its own identification system, or disclose a government related identifier unless:

- it is reasonably necessary to verify the identity of an individual
- it is reasonably necessary for the organisation to fulfil its obligations to a State or Territory authority
- it is required or authorised by law or court/tribunal order
- the organisation reasonably believes that the use or disclosure is reasonably necessary for an enforcement-related activity conducted by, or on behalf of, an enforcement body
- the organisation reasonably believes the use or disclosure is necessary to lessen or prevent a serious threat to the life, health or safety of any individual or to public health or safety, and it is unreasonably or impracticable to obtain consent

- the organisation has reason to suspect that unlawful activity, or misconduct of a serious nature, that relates to the organisation's functions or activities has been, is being, or may be engaged in, and the organisation reasonably believes that the use of disclosure is necessary in order for the organisation to take appropriate action.

Note: A person's name and their Australian Business Number are not defined as identifiers under the Privacy Act.

How We Comply with This Obligation

- we do not use government-related identifiers as our primary identification system
    - where we collect and hold a government-related identifier of an individual, we will only use or disclose this personal information when:
    - it is reasonably necessary for us to fulfil our obligations to a State or Territory authority
    - we are required or authorised by law or court/tribunal order
    - the College reasonably believes that the use or disclosure is reasonably necessary for an enforcement-related activity conducted by, or on behalf of, an enforcement body
    - the College reasonably believes that the use or disclosure is necessary to lessen or prevent a serious threat to the life, health or safety of any individual or to public health or safety, and it is unreasonably or impracticable to obtain consent
- our staff are unable to enter a government-related identifier into a database and retrieve personal information based upon that identifier.

Principle 10: Quality of Personal Information

The Legal Requirement

The College must have practices, procedures and systems in place to ensure that the personal information it collects, uses, holds and/or discloses is accurate, up-to-date, complete and relevant.

The rationale behind this requirement is to prevent situations where the College may use or disclose, inaccurate, incomplete or out-of-date personal information.

How We Comply with This Obligation

We have established and effectively implemented practices, procedures and systems to ensure that the personal information the College collects, uses, holds and/or discloses is accurate, up-to-date, complete and relevant at the time the information is collected and again when the information is used or disclosed.

This is achieved by:

- conducting regular Personal Information Audits in to identify what types of personal information we receive (both solicited and unsolicited), where we store this information (for example databases, filing cabinets, computer hard drives) and how we secure it (a Personal Information Audit Template is available in the Privacy Documents section)
- ensuring personal information is collected and recorded in a consistent format, where possible, through the use of standardised forms and privacy collection notices
- ensuring updated or new personal information is promptly added to existing records
- identifying and correcting or destroying poor quality or incorrect personal information
- contacting individuals to verify the quality of personal information if there has been a lengthy period since collection
- destroying or de-identifying personal information that is no longer required for the primary purpose it was collected
- considering whether we are using personal information for a “secondary purpose” and assessing the quality of this information
- providing training to our staff outlining our expectations with respect to the management of personal information
- providing individuals with a simple means to review and update their personal information
- ensuring that third parties collecting personal information have appropriate data quality collection/recording practices, procedures and systems
- regularly reviewing our personal information management practices, procedures and systems.

Principle 11: Security of Personal Information

The Legal Requirement

The College must take active measures to protect personal information from misuse, interference, loss, unauthorised access, modification or disclosure.

Terminology

The following terminology is used when referencing the security of personal information:

Hold: extends beyond physical possession of a record to include a record that the College has the right or power to deal with. For example, if we have outsourced storage to a third party but we retain the right to deal with the information, including to access and amend it, we will hold the information.

Interference: with personal information occurs where there is an attack on personal information that the College holds that interferes with the personal information but does not necessarily modify its content. For example, an attack on a computer system, that, for example, leads to exposure of personal information.

Loss: covers the accidental or inadvertent loss of personal information held by the College. This includes physical loss or electronic loss, for example a failure to keep adequate backups of personal information in the event of a systems failure. Loss may also occur as a result of theft following unauthorised access or modification of personal information as a result of natural disasters. The intentional destruction or de-identification of personal information by the College does not amount to loss.

Misuse: occurs when personal information is used by the College for a purpose that is not permitted by the Privacy Act.

Unauthorised access: occurs when personal information held by the College is accessed by someone who is not permitted to do so, including by an employee or external third party.

Unauthorised modification: occurs when personal information held by the College is altered by someone who is not permitted to do so, or is altered in a way that is not permitted under the Privacy Act, including by an employee or external third party.

Unauthorised disclosure: occurs when the College makes personal information accessible or visible to others outside of the College and releases the information from its effective control in a way prohibited by the Privacy Act, including by a College employee.

How We Comply with This Obligation

Security Practices, Procedures and Systems

The College has developed practices, procedures and systems relating to the security of personal information we hold, which are designed to prevent the misuse, interference, loss, modification or disclosure of personal information.

These practices, procedures and systems which have been developed having regard to the Guide to Securing Personal Information published by the OAIC include:

- appointment of designated individuals who are primarily responsible for managing and protecting the integrity of the personal information the College collects. These individuals are

allocated specific tasks to ensure our compliance with privacy laws and these tasks are monitored through CompliSpace Assurance.
- conducting regular audits of how we store and secure personal information
- ensuring personal information (in particular financial information and sensitive information such as health records) that is stored in hard copy form, is stored securely in lockable filing cabinets
- the use of security and alarm systems to ensure the security of physical files and computer systems containing personal information
- the installation of up-to-date Information and Communications Technology (ICT) security software to protect the College's computer networks, websites, web-based applications and electronic devices from malicious software (or malware), computer viruses and other harmful programs and unauthorised access
- the use of passwords enabling only authorised persons to access the College's ICT systems on a need-to-know basis
- the use of intrusion detection systems to monitor our ICT systems for malicious activities, policy violations and anomalous behaviour
- the regular monitoring and testing of our College's ICT security systems
- the backup of personal information held on our ICT systems to protect against the loss of personal information
- the implementation of policies that are designed to ensure that any staff who are required to take personal information outside College grounds, or have personal information accessible through a laptop computer or mobile device, are required to ensure the maintenance of confidentiality (especially with respect to sensitive information).

Managing Data Breaches

In the event of a breach of personal information, the College will follow our Procedures for Responding to and Reporting Data Breaches.

Destroying or De-Identifying Personal Information

If the College no longer requires personal information it holds, it will destroy or de-identify the information. If de-identified personal information is of further value or utility to the College, then the information does not need to be destroyed because that information is no longer personal information.

If held in hard copy form, the information is destroyed through a secure process of document destruction.

If held in electronic form, steps are taken to irretrievably destroy the information or put it 'beyond use'.

If held by a third party, such as a Cloud Based Service Provider, our College will instruct the third party to delete the personal information and to verify that deletion has occurred.

Principle 12: Access to Personal Information

The Legal Requirement

Individuals have the right of access to any personal information we hold about them. There are some limited exceptions to this right of access including where access would:

- be unlawful
- pose a serious threat to the life or health of another individual
- unreasonably impact on the privacy of others
- require us to disclose evaluative information in connection with a commercially sensitive matter
- adversely impact an internal investigation into unlawful activities
- be considered frivolous or vexatious
- reveal our intentions in relation to negotiations with the individual in such a way as to prejudice those negotiations
- involves legally privileged information during legal proceedings.

Where a request for access to personal information is made we must respond within a reasonable time. If access is denied we must give:

- written notice for the reasons for refusal (except where it would be unreasonable to do so)
- the mechanisms available to complain about the refusal.

The Privacy Act allows the College to impose a charge that is designed to cover costs, however this charge must not be excessive and we must disclose this charge to the individual upfront. Where access can be given, we must endeavour to provide it in a manner that is as prompt, uncomplicated and as inexpensive as possible.

How We Comply with This Obligation

The College has established a standard procedure for Dealing with Privacy Questions and Complaints.

Requests for access to personal information are referred to the College's Privacy Officer who will consider each request on its merits, having consideration to the various exemptions with respect to

the rights of the individual, and respond appropriately within a reasonable timeframe.

In considering requests for access to personal information, we take the view that a parent/carer is entitled to have access to records relating to their child, unless the child is over the age of 18 or special circumstances arise.

Principle 13: Correction of Personal Information

The Legal Requirement

The College must take reasonable steps to correct personal information where we become aware that the information we hold is inaccurate, out-of-date, incomplete, irrelevant or misleading, either as a result of our own internal activities, systems and procedures, or if we are requested to do so by an individual.

Effective compliance with other APPs, such as Principle 10: Quality of Personal Information and Principle 11: Security of Personal Information, facilitates compliance with Principle 13: Correction of Personal Information and minimises the likelihood that individuals will request us to correct their personal information.

If the College has disclosed information to another organisation, we must take reasonable steps to notify the other organisation of any corrections we make where the individual has requested us to do so.

If an individual requests that a correction be made, and we refuse that request, we must provide written reasons for the refusal and information as to how the individual can complain about the refusal.

If the College refuses a correction request and the individual requests a statement to be placed with the information that states the individual believes the information to be incorrect, we must take reasonable steps to do so in such a way that ensures that any users of the information are aware of the individual's position.

We must action corrections within a reasonable period and we must not charge for making corrections.

How We Comply with This Obligation

The College is committed to taking reasonable steps to ensure the personal information we hold is accurate, up-to-date, complete, relevant and not misleading, and we have established internal systems

and procedures for correcting personal information. These include:

- asking parents/carers to confirm the accuracy of their child's health information on a regular basis
- asking parents/carers to confirm/provide information with respect to their child's abilities (for example swimming) prior to attending an excursion
- training staff to recognise the importance of maintaining up-to-date personal information
- effective database management including the investigation and correction of bounced emails, returned letters and incorrect telephone numbers.

Reasonable steps will depend on considerations that include:

- the sensitivity of the personal information
- the possible adverse consequences for an individual if notice is not provided to another entity
- the nature or importance of the correction.

The College has established a standard procedure for Dealing with Privacy Questions and Complaints which includes dealing with requests for correction of personal information.

Simple requests for correction of personal information will be dealt with directly by staff (for example a request to update a student's address or a contact telephone number).

Any correction requests that are potentially contentious are referred to the College's Privacy Officer who will consider each request on its merits.

In all cases where a correction request is made, the College will:

- respond in a timely manner (usually within 30 calendar days)
- ensure any other entities who received the personal information through disclosure are informed of the correction
- not charge the individual for making a request, correcting personal information or associating a statement
- give notice to an individual, including reasons and available complaint mechanisms, if the correction is refused.

Health Information and Confidentiality

This section of our Privacy Program includes:

Privacy and Health Information

The College deals with health information and provides a health service.

Health Information

“Health information” is a defined term under the Privacy Act and includes information, or an opinion, about:

- the health, disability or injury (at any time) of an individual
- a “health service” to be provided to an individual
- an individual's expressed wishes about the future provision of health services
- genetic information that is, or could be, predictive of the health of the individual or a genetic relative of the individual.

It is the College's policy to treat health information as including information about an individual’s mental health.

Health Service

“Health Service” is also a defined term. Health Service means:

- an activity performed in relation to an individual, that is intended or claimed (expressly or otherwise) by the individual, or the person performing it:
    - to assess, record, maintain, improve or manage the individual's health
    - to diagnose the individual's illness, injury or disability
    - to treat the individual's illness, injury or disability or suspected illness, injury or disability
- dispensation on prescription of a drug or medicinal preparation by a pharmacist.

Collection of Health Information

In most circumstances, the College is required to collect health information in order to comply with our obligation to exercise our duty of care to students. As such we do not require specific written consent.

In most cases consent to collection will be implied, as the health information will be provided directly by a parent/carer, or a student, in response to a request for health information, or by way of

explanation with respect to a particular health problem that has arisen.

There may, however, be some occasions where we should seek specific consent to the collection of health information, especially where we are collecting health information directly from a third party, such as a doctor or another school.

Use or Disclosure of Health Information

Any health information that the College has collected must only be used or disclosed:

- for the primary purpose it was collected or for a directly related secondary purpose
- to exercise our duty of care
- to lessen or prevent a serious threat to the life, health or safety of an individual and where it is impractical to obtain consent.

To this end the College and our staff take steps to:

- secure all health information we collect
- ensure this information is only disclosed to staff on a need-to-know basis
- ensure this information is not disclosed to other students, parents or third parties without consent.

College Counsellor

Arethusa College engages an external counsellor service at the College. The College has entered into a written agreement with the service provider which governs the terms of this relationship and requires students and/or their parents/carers to provide consent for the service to share information on a need-to-know basis with members of the College staff.

Confidentiality of Personal Information

Confidentiality can be claimed in respect of personal information where:

- the information is by its nature confidential
- the information is communicated in circumstances importing an obligation of confidence
- disclosure of the information would be unauthorised by the provider of the information or by law.

As confidential information is not defined under the Privacy Act, it is the College's policy that records of confidential information should only be made where there is a need to do so and in the knowledge

that access to the record may be sought.

The College may disclose confidential information where:

- the individual consents to disclosure
- the subject of the information has requested access
- disclosure is otherwise required or authorised by law (refer to Principle 6: Use or Disclosure of Personal Information).

Refer to our Privacy Collection Notice.

Privacy for Students, the Community and Related Bodies

This section of our Privacy Program includes:

- Personal Information of Students
- Privacy and the College Community
- Transfers Between Related Bodies Corporate

Personal Information of Students

State/Territory Child Protection Regimes Override Privacy Requirements

Information sharing regimes under state/territory legislation relating to child protection override the privacy requirements under the Privacy Act.

For more information, refer to our Child Protection Program.

The College takes a common-sense approach to dealing with a student's personal information. We will determine on a case-by-case basis whether a student under the age of 18 has the capacity to consent and make decisions in respect of their personal information, and will be guided by the below principles when making any determination regarding student consent.

Consent from Parents/Carers

The College generally takes the view that notifications provided to parents/carers will act as notifications to students and consents received from parents/carers will act as consents given by students. This view is based on the fact that parents/carers generally have the right to make

decisions for their children until they reach 18 years of age and that the College's contractual relationship is with a student's parents/carers.

Consent from Students

In certain circumstances, it will be appropriate to seek and obtain consents directly from students.

As a general principle, a student under the age of 18 has capacity to consent when they have sufficient understanding and maturity to understand what is being proposed. In some circumstances, it may be appropriate for a parent/carer to consent on behalf of a student, for example if the student is very young or lacks the maturity or understanding to do so themselves.

If it is not practicable or reasonable for the College to assess the capacity of students on a case-by-case basis, we are entitled to presume that a student aged 15 or over has capacity to consent, unless there is something to suggest otherwise. Students aged under 15 are presumed to not have capacity to consent.

Student Access to Personal Information

Where a student seeks access to their personal information, the College will consider whether to refuse or restrict access, taking into account whether:

the record of personal information contains information which would not normally be released

- access is likely to adversely impact on the student
- a parent/carer of the student seeking access does not consent to their child having access.

For more information, refer to Principle 12: Access to Personal Information.

Disclosure of Student Information

Our Student Enrolment Form sets out how we collect and disclose the personal information of students, including sensitive information. Students' personal information is theirs, regardless of their age. It may hence only be disclosed to parents/carers if:

- disclosure is for the primary purpose of collection or for a related secondary purpose which is reasonably expected
- disclosure is necessary to fulfil the College's duty of care to the student.

Students may attempt to claim a right to prevent disclosure of personal information to a parent/carer, such as their College Report. Situations where a student makes a request that personal information

(particularly sensitive information) not be disclosed to parents/carers will be dealt with on a case-by-case basis.

Privacy and the College Community

The College community consists of staff, students, parents/carers, alumni, neighbours, other schools, benefactors and other stakeholders. Arethusa College has implemented the following procedures to comply with the APPs when information is shared in the College community.

College Directories

The use of College directories and class lists, which contain the names, contact details and other information of students and their parents/carers, may involve the disclosure of personal information.

The College will obtain the consent of parents/carers, and students if they have capacity to consent, to place their details in the College Directory or class list. Parents/carers and students are also notified about these practices through our Collection Notices.

College Publications

Publications such as newsletters and magazines usually contain personal information obtained from the individual or from external sources. While these publications might be considered to be generally available publications, they are still covered within the definition of personal information and hence must be managed in accordance with the Privacy Act.

Sensitive information (such as health information) should not be included in publications without consent.

College Libraries/Exhibitions

The definition of a record does not include anything kept in a library, art gallery or museum for the purposes of reference, study or exhibition.

Where the College intends to include personal information in a library/exhibition, the individual should be notified of the planned use and disclosure appropriately. Sensitive information (such as health information) should not be included without consent.

Disclosing Information to Other Schools

When the College is not related to a second school or other body, it cannot rely upon related body corporate exemptions in order to disclose information to them. Information should not usually be passed on to other schools without consent. However, information may be disclosed if it is for the primary purpose for which the information was collected or falls within a permitted secondary purpose. For more information, refer to Transfers Between Related Bodies Corporate.

Transfers Between Related Bodies Corporate

Arethusa College does not share information with other entities unless they are “related bodies corporate”, or the information is being shared for the primary purpose for which it was collected, or for a permitted secondary purpose (refer to Principle 6: Use or Disclosure of Personal Information).

Related Bodies Corporate

Under the Privacy Act, related bodies corporate (as defined in the Corporations Act) are able to share and transfer an individual’s personal information (but not sensitive information) without the share or transfer amounting to an interference with the privacy of the individual. In general terms companies are related where they have a shared controlling interest. The related bodies corporate must comply with the APPs and the CR Code (if applicable) when using or holding the personal information.

This provision covering information transfers between related bodies corporate highlights the fact that Arethusa College is not able to simply share information with other entities unless they are “related”, or there is a reasonable expectation that this information would be shared for a secondary purpose. (Refer to Principle 6: Use or Disclosure of Personal Information).

Unrelated Bodies Corporate

Currently Arethusa College have not identified any unrelated bodies corporate.

Procedures for Responding to and Reporting Data Breaches

A data breach can take many forms and have many causes. The breach may involve human error, a system fault or a deliberate hacking of a database. Depending on the circumstances of the incident, the extent of interference with personal information will vary, as will the harm suffered by the individuals affected by the interference.

Our legal obligations for reporting an incident can vary depending on the circumstances of the incident.

Arethusa College has established the following work systems, practices, policies and procedures for responding to and reporting suspected and actual data breaches both internally and externally. This includes:

- Terminology
- Guide to Data Breach Identification
- Remedial Action
- Data Breach Response Team
- Data Breach Response Plan

The Guide to Data Breach Identification which is designed to assist our staff in making decisions with respect to identifying different data breaches and when a breach will be a Notifiable Data Breach.

The Privacy Officer must be notified of any data breach.

Terminology

Data Breach

It is important to note that although the Privacy Act regulates the handling of personal information, not "data", the OAIC uses the term data breach rather than "personal information security breach" in its guidance to organisations on how to respond to an incident.

A data breach occurs when personal information held by Arethusa College is misused, interfered with, lost or subject to unauthorised access, modification or disclosure. In other words, a data breach may occur as a result of a failure by Arethusa College to protect the security of:

- personal information, in accordance with Principle 11: Security of Personal Information; and/or
- credit information, in accordance with the Privacy Act and Credit Reporting Code (the College is not a Credit Provider).

Examples of data breaches include:

- lost or stolen laptops, removable storage devices, or paper records containing personal information
- databases containing personal information being 'hacked' or otherwise illegally accessed by individuals outside of the College

- employees accessing or disclosing personal information outside the requirements or authorisation of their employment
- paper records stolen from insecure recycling or garbage bins
- the College mistakenly providing personal information to the wrong person, for example by sending details to the wrong address.

Data breaches that are likely to result in serious harm to any of the individuals to whom the information relates may be a Notifiable Data Breach.

Likely means 'more probable than not'.

Notifiable Data Breach

A Notifiable Data Breach occurs where the College holds personal information relating to one or more individuals, is required to comply with Principle 11: Security of Personal Information in relation to that information, and:

- there is unauthorised access to or disclosure of information, and a reasonable person would conclude that this 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 unauthorised access to or disclosure of information is likely to occur, and a reasonable person would conclude that, assuming this were to occur, it would be likely to result in serious harm to any of the individuals to whom the information relates.

Under the Privacy Act, these types of data breaches are referred to as "eligible data breaches", however for the purposes of this policy, the College has adopted the phrase Notifiable Data Breach as in the OAIC's guidance materials.

Serious Harm

This term is not defined in the Privacy Act. The term could include serious physical, psychological, emotional, economic and financial harm, as well as serious harm to reputation.

The Act sets out a list of factors to consider when determining whether a reasonable person would conclude that an incident of access to, or a disclosure of, information:

- would be likely; or
- would not be likely,

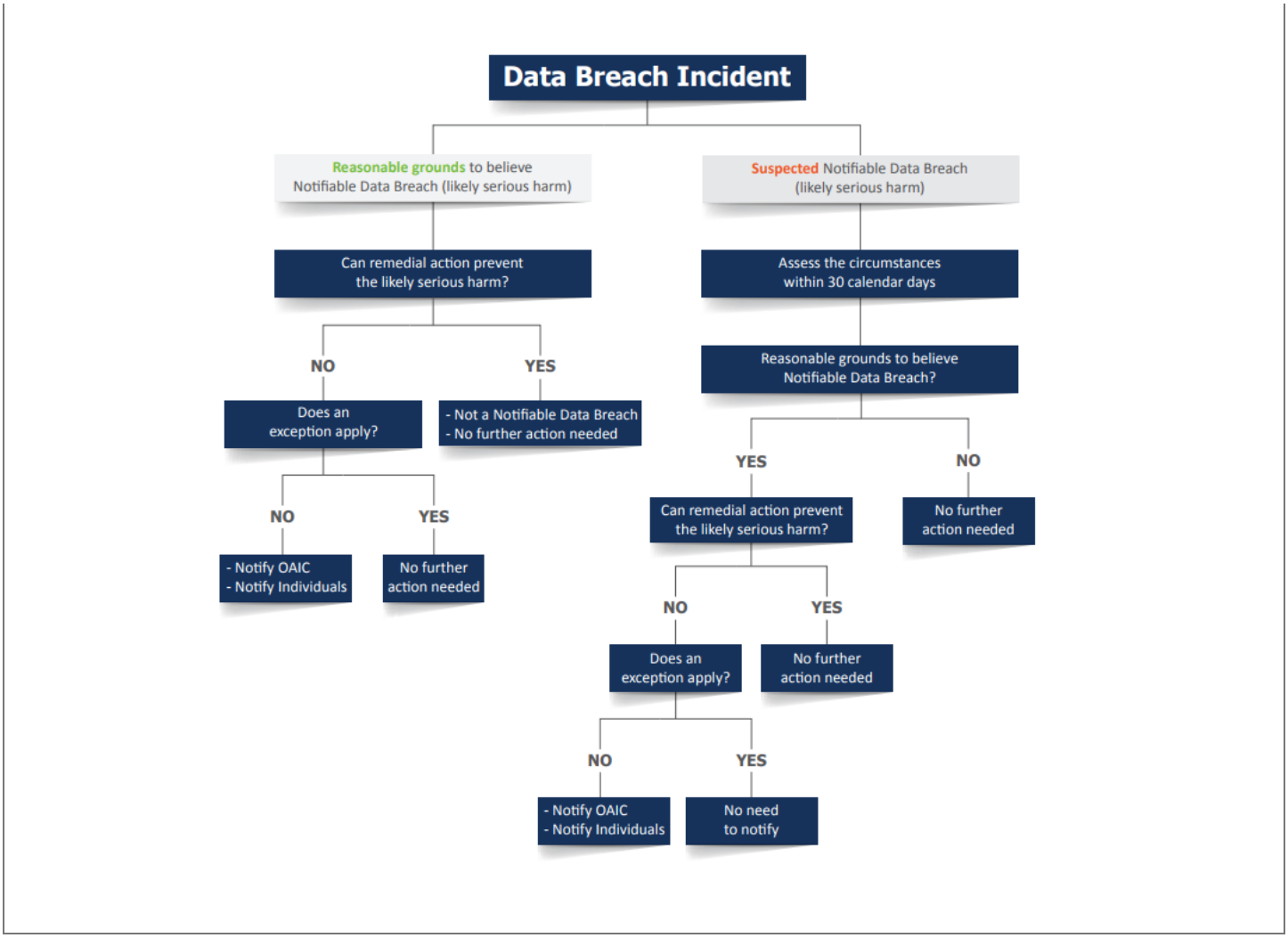
to result in serious harm to any of the individuals to whom the information relates.

Those factors are:

- the kind/s of information
- the sensitivity of the information
- whether the information is protected by one or more security measures
- if the information is protected by one or more security measures – the likelihood that any of those security measures could be overcome
- the persons, or the kinds of persons, who have obtained, or who could obtain, the information
- if a security technology or methodology was used in relation to the information and was designed to make the information unintelligible or meaningless to persons who are not authorised to obtain the information, the likelihood that the persons, or the kinds of persons, who:
- have obtained or, or who could obtain the information
- have, or are likely to have, the intention of causing harm to any of the individuals to whom the information relates
- have obtained, or could obtain, information or knowledge required to circumvent the security technology or methodology
- the nature of the harm
- any other relevant matters.

Guide to Data Breach Identification

Refer to Terminology for key definitions.



Remedial Action

What is Remedial Action?

Remedial action is action taken to contain a suspected data breach and to prevent the likely risk of serious harm occurring.

For example, if a staff member accidentally sends an email containing personal information to the wrong recipient, the Privacy Officer and the staff member may be able to take action to remedy the breach so that a reasonable person would conclude that the breach would likely not result in serious harm to any person to whom the information relates. Action could include recalling the email or contacting the recipient who agrees to delete the email.

Successful Remedial Action

If remedial action is successful, and the likely risk of serious harm occurring has been prevented, the breach will not amount to a Notifiable Data Breach and notification to the OAIC and affected individuals will not be required.

Unsuccessful Remedial Action

If remedial action is unsuccessful, meaning that the likely risk of serious harm occurring has not been prevented, the data breach will be a Notifiable Data Breach and, it may be appropriate for the Privacy Officer to escalate the matter to the Data Breach Response Team.

Voluntary Notification to OAIC and/or Individuals

Not all data breaches require notification to the OAIC and affected individuals. If there are reasonable grounds to suspect that there may have been a Notifiable Data Breach, we must comply with the notification requirements set out in the Privacy Act.

If a data breach is not a Notifiable Data Breach, the College is not legally required to notify the OAIC and affected individuals but may choose to do so as a matter of best practice. A decision to voluntarily notify the OAIC and/or affected individuals will be made on a case-by-case basis having regard to the following factors:

- notification as a reasonable security safeguard: to help protect information from misuse, interference or loss
- notification as openness about privacy practices: being open and transparent when something goes wrong
- notification as restoring control over personal information: where it will assist individuals to regain control of the information
- notification as a means of rebuilding public trust: where it will demonstrate to the public that the College takes its privacy obligations seriously

OAIC Contact Details:

If we decide to notify the OAIC we will do so using one of the following contact options:

- Email: enquiries@oaic.gov.au
- Telephone: 1300 363 992
- Facsimile: + 61 2 9284 9666
- Post: GPO Box 5218, Sydney NSW 2001

Data Breach Response Team

In the event of a Notifiable Data Breach, the Privacy Officer will establish a Data Breach Response Team (DBRT). The DBRT is responsible for assisting the Privacy Officer in investigating the breach and notifying the OAIC when required.

The DBRT members will include representatives from the Management Team, the College's technology team and other departments as needed.

Depending on the nature of the breach, the composition of the DBRT may vary. For example, the College is alerted to the incident through a complaint, the Complaints Manager would form part of the Team.

Data Breach Response Plan

If a data breach is identified using the Guide to Data Breach Identification, the Data Breach Response Plan must be followed.

The Data Breach Response Plan sets out procedures and clean lines of authority for the College in the event that it experiences circumstances that amount to a data breach or a Notifiable Data Breach.

The response in the Data Breach Response Plan is intended to enable the College to contain, assess and respond to data breaches in a timely fashion, to help mitigate potential harm to affected individuals and to meet our notification obligations under the Privacy Act.

Information Collecting

Various steps in the Data Breach Response Plan require the collection of information.

In the event that the Data Breach Response Plan is activated, the Privacy Officer will ensure that:

- evidence is preserved that may be valuable to determine the context of the data breach and a list of affected individuals, or possible affected individuals
- information will be compiled for external notification processes and internal reporting
- records of the information are kept.

Dealing with Privacy Questions and Complaints

Privacy inquiries or complaints are dealt with on a similar basis to any other inquiries and complaints we receive. Inquiries and complaints can arise verbally or in writing.

Verbal Privacy Inquiry or Complaint

To ensure all verbal privacy inquiries or complaints received are managed appropriately, staff must record details of the inquiry or complaint through CompliSpace Assurance.

CompliSpace Assurance assists us in capturing all of the relevant information to enable us to investigate and respond to a privacy inquiry or complaint. Incidents logged through CompliSpace Assurance are automatically submitted to the Privacy Officer for further action.

Handling a privacy complaint efficiently requires patience and skill to avoid an initially negative situation from escalating.

Arethusa College's Complaints Handling Program and procedures have been designed to minimise the potential for complaints to unnecessarily escalate.

Written Privacy Inquiry or Complaint

The following procedure is to be adopted where a written privacy inquiry or complaint is received:

- All written privacy inquiries or complaints must immediately be forwarded to the Privacy Officer. The Privacy Officer will review the relevant correspondence and log details of the privacy inquiry or complaint through CompliSpace Assurance.
- The person inquiring or complaining should be contacted by telephone (if possible) to acknowledge that we have received their inquiry or complaint and to obtain any additional information which may assist in resolving the matter quickly. Our guidelines relating to the management of verbal inquiries or complaints should be followed in this circumstance.
- If it is not possible to contact the person by telephone, additional information should be sought through appropriately worded written correspondence.

Privacy Training

The College recognises that without training and educating our staff, our policies and procedures will not operate to effectively protect personal information from misuse, interference, loss or unauthorised access, modification or disclosure.

Staff receive privacy training when they first commence their role at Arethusa College, and are required to complete ongoing training on privacy issues at least annually through our Privacy Training Program.

Continuous Review and Improvement

Arethusa College is committed to continuous improvement in all its operations, including this Privacy Program.

It is the responsibility of the Executive Principal to regularly review our Privacy Program for overall effectiveness and to ensure that the College is complying with all privacy related laws, regulations and guidance.

Our Privacy Documents and Additional Resources

This section of our Privacy Program includes:

- Our Privacy Documents
- OAIC Guidance Materials

Our Privacy Documents

Privacy Policy

Credit Reporting Policy

OAIC Guidance Materials

The following resources provide further information on privacy matters.

What is Personal Information

Australian Government Office of the Australian Information Commissioner, What is Personal Information?, May 2017

What is a Permitted General Situation for Use or Disclose of Personal Information?

Australian Government Office of the Australian Information Commissioner, Chapter C – Permitted general situations, February 2014

What is a Permitted Health Situation for Use or Disclosure of Personal Information?

Australian Government Office of the Australian Information Commissioner, Chapter D: Permitted health situations, February 2014

Australian Privacy Principles

Australian Government Office of the Australian Information Commissioner, APP Guidelines, March 2018

Securing Personal Information

Australian Government Office of the Australian Information Commissioner, Guide to securing personal information, June 2018

Data Breach

Australian Government Office of the Australian Information Commissioner, Data breach preparation and response - A guide to managing data breaches in accordance with the Privacy Act 1988 (Cth), February 2018

De-identification of Data and Information

Australian Government Office of the Australian Information Commissioner, De-identification and the Privacy Act, March 2018