



Privacy Policy

Executive Summary

Purpose of This Document

This document sets out to clearly articulate the policies and procedures Wycliffe Christian School employs in managing the personal information provided to, or collected by, the School. This management is undertaken for the well-being of the students in our care and to support the reasonable and essential functions of the school.

Pages in this Section

- [Christian Rationale](#)
- [Our Privacy Policy](#)
- [Key Information Related to Privacy and Personal Information](#)
- [Data Breaches Relating to Personal Information](#)



Privacy Policy

Christian Rationale

Wycliffe Christian School acknowledges its responsibility before God to care for and protect the children, families and others who trust the School to carry out those responsibilities with love and respect.

The School respects the privacy of individuals and families and places a high priority on integrity in its handling of information provided to the School. It seeks to protect the rights of all people who provide information to the school, in accordance with relevant legislation.

The School honours the Commonwealth and State laws which circumscribe the collection, storage and dissemination of information provided to it.



Privacy Policy

Our Privacy Policy

Scope of Policy and Source of Obligation

In the course of Wycliffe Hope School's activities, we manage and protect personal information in accordance with the Privacy Act 1988 (Cth) (Privacy Act) and the 13 Australian Privacy Principles (APPs).

In addition to these, we also comply with the requirements of relevant state-based legislation, including the Health Records and Information Privacy Act 2002.

Scope of Policy

This policy outlines the circumstances in which we obtain personal information, how we use and disclose that information and how we manage requests to access and/or change that information.

What is Personal Information and How Do We Collect Personal Information?

Personal information is information, or an opinion about an individual, from which they can be reasonably identified. Depending on the circumstances, we may collect personal information from the individual in their capacity as a student, contractor, volunteer, stakeholder, job applicant, alumni, visitors or others that come into contact with the School.

In the course of providing services we may collect and hold:

- Personal Information including names, addresses and other contact details; dates of birth; next of kin details; photographic images; attendance records and financial information.

- Sensitive Information (particularly in relation to student and parent records) including government identifiers (such as Tax File Numbers), religious beliefs, nationality, country of birth, professional memberships, family court orders and criminal records.
- Health Information (particularly in relation to student and parent records) including medical records, disabilities, immunisation details and psychological reports.

As part of our recruitment processes for employees, contractors and volunteers, we may collect and hold:

- Personal Information including names, addresses and other contact details, dates of birth, financial information, citizenship, employment references, regulatory accreditation, media, directorships, property ownership and driver's licence information.
- Sensitive Information including government identifiers (such as TFN), nationality, country of birth, professional memberships, family court orders and criminal records.
- Health Information (particularly in relation to prospective staff and student records) including medical records, disabilities, immunisation details and psychological reports.

Generally, we will seek consent from the individual in writing before we collect their sensitive information (including health information).

It is noted that employee records are not covered by the APPs where they relate to current or former employment relations between the School and the employee.

However, a current or former employee's health records are covered by the NSW Health Privacy Principles.

Collection of Personal Information

The collection of personal information depends on the circumstances in which Wycliffe Hope School is collecting it. If it is reasonable and practical to do so, we collect personal information directly from the individual.

Solicited Information

Wycliffe Hope School has, where possible, attempted to standardise the collection of personal information by using specifically designed forms (e.g. an Enrolment Form or Health Information Disclosure Form). However, given the nature of our operations we may also receive personal information by email, letters, notes, via our website, over the telephone, in face-to-face meetings,

through financial transactions and through surveillance activities such as the use of CCTV security cameras or email monitoring.

We may also collect personal information from other people (e.g. a third-party administrator, referees for prospective employees) or independent sources. However, we will only do so where it is not reasonable and practical to collect the personal information from the individual directly.

Information Collected from Our Website

We may collect information based on how individuals use our website. We use “cookies” and other data collection methods to collect information on website activity such as the number of visitors, the number of pages viewed and the internet advertisements which bring visitors to our website. This information is collected to analyse and improve our website, marketing campaigns and to record statistics on web traffic. We do not use this information to personally identify individuals.

Unsolicited Information

Wycliffe Hope School may be provided with personal information without having sought it through our normal means of collection. This is known as unsolicited information and is often collected by:

- misdirected postal mail – letters, notes, documents
- misdirected electronic mail – emails, electronic messages
- employment applications sent to us that are not in response to an advertised vacancy
- additional information provided to us which was not requested.

Unsolicited information obtained by Wycliffe Hope School will only be held, used and/or disclosed if it is considered as personal information that could have been collected by normal means. If that unsolicited information could not have been collected by normal means then we will destroy, permanently delete or de-identify the personal information as appropriate.

Collection and Use of Sensitive Information

We only collect sensitive information if it is:

- reasonably necessary for one or more of these functions or activities, and we have the individual’s consent
- necessary to lessen or prevent a serious threat to life, health or safety
- another permitted general situation

- another permitted health situation.

We may share sensitive information to other entities in our organisation structure, but only if necessary, for us to provide our products or services.

How Do We Use Personal Information?

Wycliffe Hope School only uses personal information that is reasonably necessary for one or more of our functions or activities (the primary purpose) or for a related secondary purpose that would be reasonably expected by you, or for an activity or purpose to which you have consented.

Our primary uses of personal information include, but are not limited to:

- providing education, pastoral care, extra-curricular and health services
- satisfying our legal obligations including our duty of care and child protection obligations
- keeping parents informed as to School community matters through correspondence, newsletters and magazines
- marketing, promotional and fundraising activities
- supporting the activities of School associations
- supporting the activities of the School
- supporting community based causes and activities, charities and other causes in connection with the School's functions or activities
- helping us to improve our day-to-day operations including training our staff
- systems development, developing new programs and services, undertaking planning, research and statistical analysis
- School administration including for insurance purposes
- the employment of staff
- the engagement of volunteers.

We will only use or disclose sensitive or health information for a secondary purpose if you would reasonably expect us to use or disclose the information and the secondary purpose is directly related to the primary purpose.

We may share personal information to related bodies corporate, but only if necessary, for us to provide our services.

The School may disclose information about an individual to overseas recipients only when it is necessary, for example to facilitate a student exchange program. The School will not however send

information about an individual outside of Australia without their consent.

Storage and Security of Personal Information

Wycliffe Hope School stores Personal Information in a variety of formats including, but not limited to:

- databases
- hard copy files
- personal devices, including laptop computers
- third party storage providers such as cloud storage facilities
- paper based files.

Wycliffe Hope School takes all reasonable steps to protect the personal information we hold from misuse, loss, unauthorised access, modification or disclosure.

These steps include, but are not limited to:

- restricting access and user privilege of information by staff depending on their role and responsibilities
- ensuring staff do not share personal passwords
- ensuring hard copy files are stored in lockable filing cabinets in lockable rooms. Staff access is subject to user privilege
- ensuring access to Wycliffe Hope School's premises is secured at all times.
- implementing physical security measures around the School buildings and grounds to prevent break-ins
- ensuring our IT and cyber security systems, policies and procedures are implemented and up to date
- ensuring staff comply with internal policies and procedures when handling the information
- undertaking due diligence with respect to third party service providers who may have access to personal information, including customer identification providers and cloud service providers, to ensure as far as practicable that they are compliant with the apps or a similar privacy regime
- the destruction, deletion or de-identification of personal information we hold that is no longer needed or required to be retained by any other laws.

Our public website may contain links to other third-party websites outside of Wycliffe Hope School.

Wycliffe Hope School is not responsible for the information stored, accessed, used or disclosed on such websites and we cannot comment on their privacy policies.

Responding to Data Breaches

Wycliffe Hope School will take appropriate, prompt action if we have reasonable grounds to believe that a data breach may have or is suspected to have occurred. Depending on the type of data breach, this may include a review of our internal security procedures, taking remedial internal action, notifying affected individuals and the Office of the Australian Information Commissioner (OAIC). For more information refer to [Notifiable Data Breaches](#).

If we are unable to notify individuals, we will publish a statement on our website and take reasonable steps to publicise the contents of this statement.

Disclosure of Personal Information

Personal information is used for the purposes for which it was given to Wycliffe Hope School, or for purposes which are directly related to one or more of our functions or activities.

Personal information may be disclosed to government agencies, other parents, other schools, recipients of School publications, visiting teachers, counsellors and coaches, our services providers, agents, contractors, business partners, related entities and other recipients from time to time, if the individual:

- has given consent; or
- would reasonably expect the personal information to be disclosed in that manner.

Wycliffe Hope School may disclose personal information without consent or in a manner which an individual would reasonably expect if:

- we are required to do so by law
- the disclosure will lessen or prevent a serious threat to the life, health or safety of an individual or to public safety
- another permitted general situation applies
- disclosure is reasonably necessary for a law enforcement related activity
- another permitted health situation exists.

Disclosure of Personal Information to Overseas Recipients

Personal information about an individual may be disclosed to an overseas organisation in the course of providing our services, for example when storing information with a “cloud service provider” which

stores data outside of Australia.

We will however take all reasonable steps not to disclose an individual's personal information to overseas recipients unless:

- we have the individual's consent (which may be implied)
- we have satisfied ourselves that the overseas recipient is compliant with the APPs, or a similar privacy regime
- we form the opinion that the disclosure will lessen or prevent a serious threat to the life, health or safety of an individual or to public safety
- we are taking appropriate action in relation to suspected unlawful activity or serious misconduct.

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.

At Wycliffe Hope School we take a pragmatic approach to dealing with a student's personal information and generally 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 students and we will treat consents provided by parents/carers as consents provided by a student.

We are, however, cognisant of the fact that children do have rights under the Privacy Act, and that in certain circumstances (especially when dealing with older students and especially when dealing with sensitive information), it will be appropriate to seek and obtain consents directly from students. We also acknowledge that there may be occasions where a student may give or withhold consent with respect to the use of their personal information independently from their parents/carers.

There may also be occasions where parents/carers are denied access to information with respect to their children, because to provide such information would have an unreasonable impact on the privacy of others, or result in a breach of the School's duty of care to the student.

The Quality of Personal information

We take all reasonable steps to ensure the personal information we hold, use and disclose is accurate, complete and up-to-date, including at the time of using or disclosing the information.

If the School becomes aware that the personal information is incorrect or out of date, we will take reasonable steps to rectify the incorrect or out of date information.

Access and Correction of Personal Information

You may submit a request to us to access the personal information we hold, or request that we change the personal information. Upon receiving such a request, we will take steps to verify your identity before granting access or correcting the information.

If we reject the request, you will be notified accordingly. Where appropriate, we will provide the reason/s for our decision. If the rejection relates to a request to change personal information, an individual may make a statement about the requested change and we will attach this to their record.

Complaints

You can make a complaint about how the School manages personal information, including a breach of the APPs by notifying us in writing as soon as possible. We will respond to the complaint within a reasonable time (usually no longer than 30 days) and we may seek further information in order to provide a full and complete response.

Wycliffe Hope School does not charge a fee for the handling of complaints.

If you are not satisfied with our response, you may refer the complaint to the OAIC. A complaint can be made using the OAIC online [Privacy Complaint form](#) or by mail, fax or email. A referral to OAIC should be a last resort once all other avenues of resolution have been exhausted.

How to Contact Us

The School can be contacted about this Privacy Policy or about personal information generally, by:

- emailing privacy@wycliffe.nsw.edu.au or business@wycliffe.nsw.edu.au
- calling (02) 4753 6422
- writing to our Privacy Officer at privacy@wycliffe.nsw.edu.au or 133 Rickard Road, Warrimoo NSW 2774.

If practical, you can contact us anonymously (i.e. without identifying yourself) or by using a pseudonym. However, if you choose not to identify yourself, we may not be able to give you the information or provide the assistance you might otherwise receive if it is not practical to do so.

Changes to Our Privacy and Information Handling Practices

This Privacy Policy is subject to change at any time.

Please visit our Privacy Policy on our website regularly for any changes.

This Privacy Policy was last reviewed: June 2025



Privacy Policy

Key Information Related to Privacy and Personal Information

This section covers key information for staff about privacy obligations.

Pages in this Section

- [Key Privacy Contacts](#)
- [What is a Data Breach?](#)
- [What is Personal Information?](#)
- [Whose Information is Protected by the Privacy Act?](#)
- [How Information is Protected - Australian Privacy Principles \(APP\) Overview](#)
- [Student Information](#)
- [Employee Information](#)
- [Source of Obligations](#)



Privacy Policy

Key Privacy Contacts

Our Privacy Officer

David Johnston is our Privacy Officer.

Our Privacy Officer can be contacted at:

- privacy@wycliffe.nsw.edu.au
- (02) 4753 6422

Our Privacy Officer is the first point of contact for advice on privacy matters related to the School:

- our privacy policy
- our procedures for protecting privacy
- requests to access personal information
- complaints regarding privacy.



Privacy Policy

What is a Data Breach?

A data breach occurs when personal information is lost, stolen or accessed or disclosed without authorisation.

Examples of breaches include:

- mis-sent emails
- lost or stolen laptops, USBs, smart devices or hardcopy files
- hacking, phishing,
- misuse of personal information
- unauthorised access
- unauthorised disclosure to either specific third parties or published generally (for example including an identifiable image of a person on a website without their consent).

If you become aware of a data breach you must immediately contact:

the Principal or Business Manager

The key priority is to remediate the breach if possible.

Notifiable Data Breach

If a data breach has not been remedied and it is likely to result in serious harm to an affected individual or affected individuals, then the affected individuals must be advised promptly and the Office of the Australian Information Commissioner (OAIC) must be notified. Serious harm can mean physical, psychological, social, financial or reputational.



Privacy Policy

What is Personal Information?

Personal Information

Personal information in the Privacy Act 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
- images
- 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 disc
- 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). Protection of business information is addressed under confidentiality requirements.
- information that has been de-identified.

Health information about persons who have been deceased for a period of 30 years or less is considered to be personal information for the purposes of the HRIP Act. Health information of persons who have been deceased for more than 30 years, and all other information about deceased persons, is not considered to be personal information in NSW.

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.



Privacy Policy

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 School.

An individual must be identified or reasonably identifiable for information to constitute personal information^{**}.^{**}

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

- 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 School employees. As noted below, the exemption for employees only relates to employee records used directly in the context of the employment relationship. Once a person becomes an employee their employee records are exempt from the application of the Privacy Act.

The School 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 School Board
- volunteers
- donors
- members of the local community.



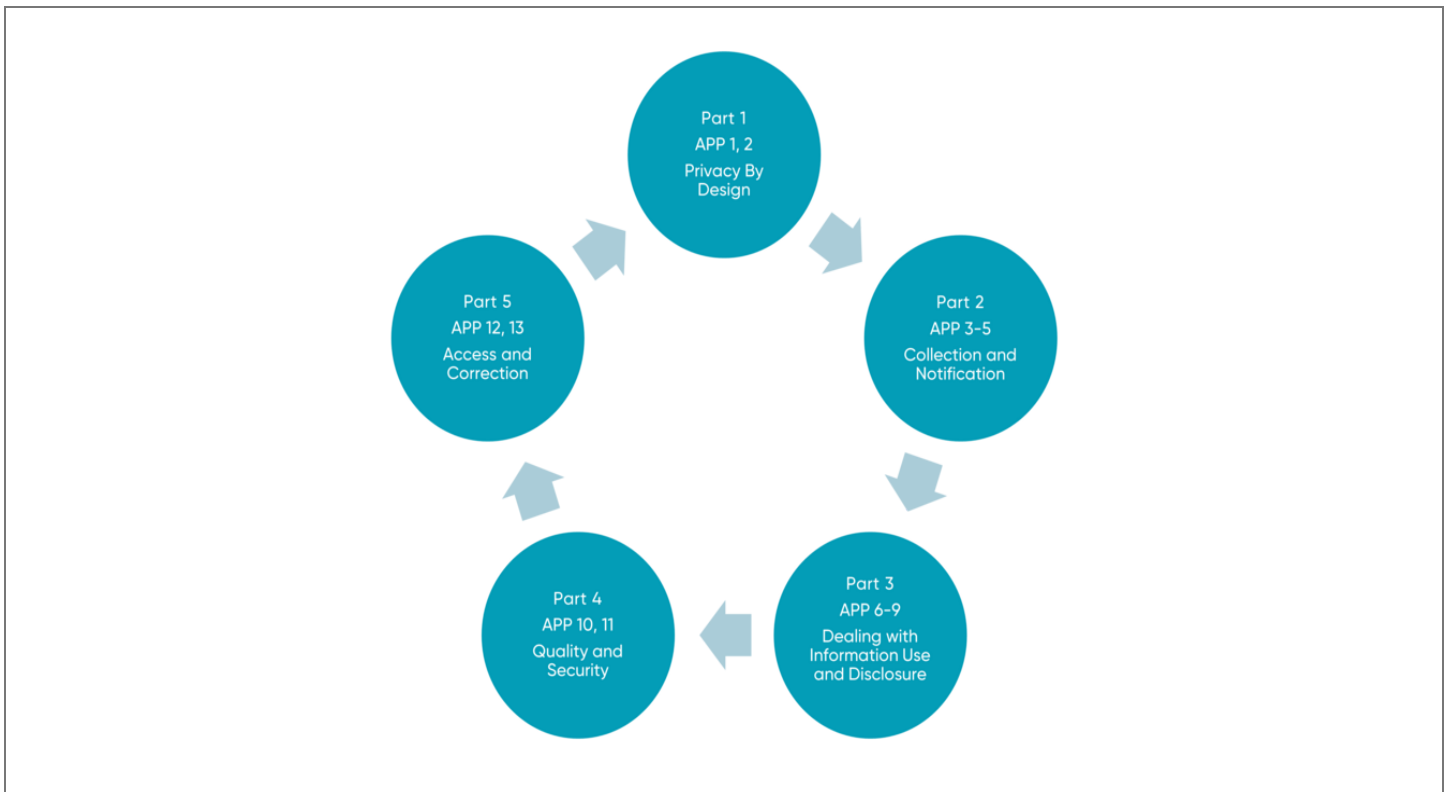
Privacy Policy

How Information is Protected - Australian Privacy Principles (APP) Overview

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

Part 4 – Information Quality and Security of Information

Principle 10: Quality of Personal Information

Principle 11: Security of Personal Information

Part 5 – Access to and Correction of Information

Principle 12: Access to Personal Information

Principle 13: Correction of Personal Information

Further information is available from the [Office of the Australian Information Commissioner](#).



Privacy Policy

Student Information

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.

The OAIC advises that 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 School 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.

The School's decisions relating to a student's personal information will be affected by the School's duty of care, role of parents/carers, and child safety information-sharing legislation.



Privacy Policy

Employee Information

The Privacy Act does not apply to acts or practices relating to employee records of an individual if the acts or practices directly relate to a current or former employment relationship between the employer and the individual.

An "employee record" 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 that is exempt from the application of the APPs.

The Privacy Act still applies to:

- employees that are employed through another corporation (e.g. contract teachers)
- employee records that are provided to a third party such as an industry association, educational authority, external training provider, recruiter or payroll service.

- personal information collected from prospective employees who are subsequently not employed by the School, such as unsuccessful job applicants or individuals who send in unsolicited curriculum vitae
- volunteers
- contractors and sub-contractors.
- information that does not relate directly to the employment relationship (this may be determined on a case-by-case basis).

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.

Workplace Surveillance and Privacy

Different types of workplace surveillance such as monitoring email, internet and other computer resources, GPS/tracking devices, CCTV and phone surveillance which collect employees' personal information, will generally be exempt from the application of the Privacy Act. However, work-related surveillance is addressed in some federal, state and territory-based legislation, and additional conditions will apply, such as strict advance notice of monitoring requirements, and clear policies advising employees of the purpose and use of the information collected.



Privacy Policy

Source of Obligations

Privacy Act 2014 (Cth) including the 13 Australian Privacy Principles

Privacy Regulation 2013 (Cth)

In NSW, the Health Records and Information Privacy Act 2002 (NSW) (HRIP Act) also applies to schools that collect, hold, use or disclose a person's health information.

Wycliffe Hope School is required to comply with both the HRIP Act for information it holds on health matters, and the Privacy Act for other personal information (including sensitive information and health information).



Privacy Policy

Data Breaches Relating to Personal Information

Data Breaches

A data breach may occur as a result of malicious action (by an external or insider party), human error, or a failure by Wycliffe Hope School in regard to the proper handling or security of personal information.

If you become aware of a data breach you must immediately contact:

the Principal or Business Manager

The key priority is to address the breach as soon as possible, and enable action to be taken if possible, to mitigate any damage or harm.

Notifiable Data Breach

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 (also called an Eligible Data Breach).

A Notifiable Data Breach will occur if the School holds personal information relating to one or more individuals 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.

Serious harm arising from a data breach could include serious physical, psychological, emotional, economic and financial harm, as well as serious harm to reputation, of an affected individual.

Responding to and Reporting Data Breaches

If there is a Notifiable Data Breach the Privacy Act requires the School to notify any affected individuals and the Office of the Australian Information Commissioner (OAIC). The notification must also include recommendations about the steps that individuals should take in response to the data breach. Our legal obligations for reporting an incident can vary depending on the circumstances of the incident. Wycliffe Hope School 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:

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

The Guide to Data Breach Identification 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.

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 Individuals

If a data breach is not a Notifiable Data Breach, the School 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 affected individuals will be made on a case-by-case basis having regard to the following factors:

- to help individual's protect information from misuse, interference or loss eg by changing their password
- as a means of rebuilding public trust, where it will demonstrate to the public that the School 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 Plan

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

The Data Breach Response Plan sets out procedures and clear lines of authority for the School 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 School 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.

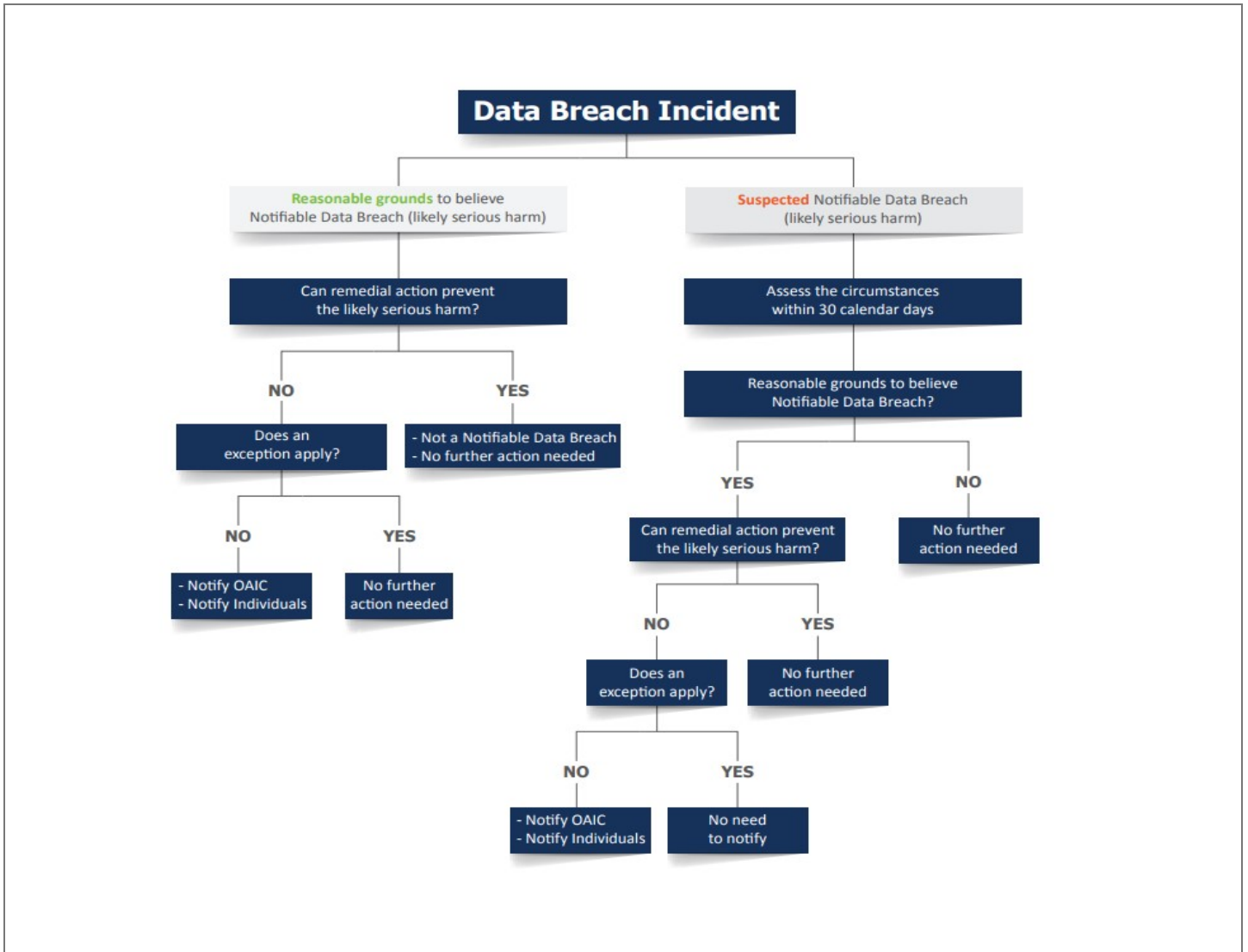
Information Collecting

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.

Guide to Data Breach Identification



Data Breach Response Plan

The OAIC has provided the following Data Breach Response Plan that the School uses:

