



## POLICIES AND PROCEDURES

information;

- d) biometric information that is to be used for the purpose of automated biometric verification or biometric identification, or
- e) biometric templates.

What type of personal information does the School collect?

The type of information that the School collects and holds will depend on the nature of a person's involvement with the School.

Depending on the reason for collecting the personal information, the personal information collected by the School may include (but is not limited to) name, residential address, email address, fax number, phone number, current employment information, Medicare and private health insurance details, superannuation fund details, personal relationships with others, next of kin details, images (including digital images for internal identification purposes), date of birth, bank account details, academic results, qualifications and Media footage of students

The School may also collect sensitive information from a person including health information, working with children checks and police records.

A person is not required to provide the personal information and/or sensitive information requested by the School, however if a person chooses not to provide information as requested, it may not be practicable for the School to service the person's needs. For instance, it will not be possible for the School to enrol a person, provide education to a person, or employ a person, if they want to remain an (,)6.9 ( i)-7.5 ( w)1.3d0.7 ( a)-3.3 ( i)-14.1 (1(r)-2.8 ( e)-6 ( m(e)-6 ( s(e)-6 ( r)-2.8 ( p)-

## POLICIES AND PROCEDURES

The School will generally obtain consent from the owner of personal information to collect their personal information. Consent will usually be provided in writing however sometimes it may be provided orally or may be implied through a person's conduct.

## POLICIES AND PROCEDURES

The purpose for which the School uses personal information of students and parents and/or guardians include:

- a) providing schooling to students;
- b) correspondence with parents and/or guardians to keep parents and/or guardians informed about matters related to their child's performance at school;
- c) publication of newsletters and articles on the website;
- d) day to day administration;
- e) looking after a student's educational, social and medical wellbeing;
- f) fulfilling its duty of care obligations;
- g) the collection of debts owed to the School;
- h) seeking donations and other fundraising activities for the School.

The School may publish the contact details of parents and/or guardians in a class list and publish

## POLICIES AND PROCEDURES

c) the disclosure is required or authorised by an Australian law or a ~~code~~.

Direct marketing

From time to time,

## POLICIES AND PROCEDURES

an annual basis and prior to school camps and excursions.

A person may contact the School at any time to update their personal information held by the School.

The School will destroy or de-identify any personal information which is no longer required by the School for any purpose for which the School may use or disclose it, unless the School is required by law or under an Australian law or a court order to retain it.

How a person can access personal information?

## POLICIES AND PROCEDURES

- otherwise complying with the Australian Privacy Principles or applicable privacy legislation.

The School may also store personal information in the 'cloud' which means that information is held on the servers or third party cloud service providers engaged by the School. Some personal information may be collected and processed or stored by these providers. These servers may be situated in or outside Australia.

The School makes reasonable efforts to be satisfied about the security of any personal information collected, processed and stored in or outside Australia.

### Notifiable data breach

A reportable major or serious data breach is one that is likely to result in serious harm to any of the affected individuals. Serious harm can include physical, psychological, emotional, financial, or reputational harm. Under the Notifiable Data Breach Scheme, such breaches must be reported to the Office of the Australian Information Commissioner (OAIC).

The OAIC does not need to be notified about data breach that does not have the potential to cause serious harm.

If the School suspects or believes that an eligible data breach has occurred, the School conduct a risk assessment of the relevant factors, as promptly as practicable, to determine if an eligible breach occurred, and take all reasonable steps to complete this assessment within 30 days of becoming aware of the breach. Examples of data breaches causing serious harm include:

- Loss or theft of School laptop or other electronic device containing the personal information of students or staff;
- Hacking of a database containing personal information;
- Loss of hard copy private confidential information;
- Mistaken provision of personal information to the wrong person.

When there is a suspected data breach reported, the School will enact the Data Breach Response Plan.

When a data breach has been identified as eligible, the School will

- Prepare and submit a statement to the OAIC in [the format prescribed](#) as soon as practicable after becoming aware of the eligible data breach;
- Take reasonable steps, in the circumstances, to contact all affected individuals directly, or
- If direct contact is not practicable, contact affected individuals indirectly by publishing information on the school's website or other publicly available forum;
- Review internal processes to identify any weaknesses to address to avoid the breach to happen again.

## POLICIES AND PROCEDURES

### Complaints

Complaints about a breach of the APPs must be made in writing and according to the School's

Complaints and Grievances Policy, available at [www.yvg.vic.edu.au](http://www.yvg.vic.edu.au). The School will investigate [figch 'p14.1\(](#)