Blackheath & Thornburgh College

PRIVACY POLICY

Document Number:	HR01_01a
Topic:	Privacy
Approval Authority:	Board of Directors
Document Owner	Principal and Business Manager
Last Approval Date:	October 2017
Review Date:	As required
Audience:	Board of Directors, Appointed Officers, Employees, Stakeholders
Related Policies	Social Media Policy, Grievance Policy, Management of Personal Information Policy
Document Web Links:	https://www.oaic.gov.au/privacy-law/privacy-archive/privacy-resources-archive/national-privacy-principles
Notes:	

Purpose

The Board Directors and other appointed Officers, employees and various stakeholders of Blackheath & Thornburgh College are bound by the Australian Privacy Principles contained in the Commonwealth Privacy Act.

The College manages personal information provided or collected by it. For information on the type of information the College collects, how the information is to be handled and disclosed, including (but not limited to) how the information may be accessed please refer to Blackheath & Thornburgh College Management of Personal Information Policy.

A source of information can be obtained from various stakeholders to Blackheath & Thornburgh College, as well as Directors and employees from time to time.

The purpose of this policy is to detail guidelines to maintain the confidentiality of such information.

Policy Details

The Information Privacy Act 2009 (Qld) (IP Act) recognises the importance of protecting the personal information of individuals. It contains a set of rules or 'privacy principles' that govern how organisations collect, store, use and disclose personal information. The IP Act also allows an individual to make a complaint about any organisations breach of the privacy principles.

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

Exemption

Under the Privacy Act, the Australian Privacy Principles do not apply to an employee record held by the employing entity. As a result, this Privacy Policy does not apply to the College's treatment of an employee record, where the treatment is directly related to a current or former employment relationship between the College and employee.

In some circumstances, a private sector College's handling of employee records in relation to current and former employment relationships is exempt from the APPs (s7B(3)).

The exemption applies if the organisation's act or practice is directly related to two things:

1. A current or former employment relationship between the College and the individual

The act or practice must directly relate to a current or former employment relationship. The exemption does not cover future employment relationships. This means that the exemption will not apply to the collection of personal information about prospective employees who are subsequently not employed by the College, such as unsuccessful job applicants. However, once an employment relationship is formed with an individual, the records the College holds relating to that individual's pre-employment checks become exempt.

This exemption does not apply to acts or practices of the College that are outside the scope of the employment relationship. *For example, a College that intends to sell a list of employees to another organisation for marketing purposes would need to comply with the APPs.*

2. An employee record held by the organisation relating to the individual

The employee record must be held by the College and must relate to the individual. An employee record is defined under *section 6(1)* to mean a record of personal information relating to the employment of the employee. Examples include health information about an employee, as well as personal information relating to:

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

The College may not be able to assume that all the information they hold that relates to an individual employee would be an employee record. For example, whilst an employee's bank details may form part of an employee record, emails an employee receives from their financial institution via their work email account may not necessarily be part of an employee record as they may not relate to the employment of the employee. Whether or not the content of emails sent or received by an employee forms part of their employee record will depend on the circumstances in any particular case.

The College endorses the ten guidelines as stated in the Privacy Principals, which are:

National Privacy Principles (NPP)

NPP 1: Collection

Describes what an organisation should do when collecting personal information, including what they can collect, collecting from third parties and, generally, what they should tell individuals about the collection.

NPP 2: Use and disclosure

Outlines how organisations may use and disclose individuals' personal information. If certain

conditions are met, an organisation does not always need an individual's consent to use and disclose personal information. There are rules about direct marketing.

NPPs 3-4: Information quality and security

An organisation must take steps to ensure the personal information it holds is accurate and up-to-date, and is kept secure from unauthorised use or access.

NPP 5: Openness

An organisation must have a policy on how it manages personal information, and make it available to anyone who asks for it.

NPP 6: Access and correction

Gives individuals a general right of access to their personal information, and the right to have that information corrected if it is inaccurate, incomplete or out-of-date.

NPP 7: Identifiers

Generally prevents an organisation from adopting an Australian Government identifier for an individual (e.g. Medicare numbers) as its own.

NPP 8: Anonymity

Where possible, organisations must give individuals the opportunity to do business with them without the individual having to identify themselves.

NPP 9: Trans-border data flows

Outlines how organisations should protect personal information that they transfer outside Australia.

NPP 10: Sensitive information

Sensitive information includes information such as health, racial or ethnic background, or criminal record. Higher standards apply to the handling of sensitive information.

Provision of Information

The College will respond to a person's written and signed request for their personal information as soon as practicable.

The time taken to respond to an employee's request for access may be influenced by various factors, and these may include the method of communication, the type or amount of personal information requested, how the personal information is held, if a third party needs to be consulted and how it is to be provided to the individual making the request.

Information will be provided to associated bodies (P&F, Foundation Committee and BPSA) from time to time as part of the College community.

Access

Requests for information will not be accepted over the telephone.

Written requests for personal information must be directed to the Human Resources Administrator, Principal or Business Manager.

Breach of the Privacy Policy

The Privacy Policy is designed to promote and enhance the confidentiality of both employees and Directors. A failure to comply with this policy will be viewed seriously and may, in line with the enterprise agreement(s) in place at the time, result in disciplinary action, including dismissal.

Both employees and Directors must report breaches of this policy to the either the Board Chairman, Company Secretary or Principal whomever is responsible for the application of legislation. The College will use its utmost endeavours to protect employees and Directors who, in good faith and with good grounds, report breaches of the privacy policy.

Grievances

Any grievance arising from the application of these arrangements shall be managed using the grievance management process foreshadowed in the College Enterprise Agreement. In the interim, any unresolved issue should be raised in the first instance with either the Principal, Business Manager and or the Company Secretary.