



- (c) investigating complaints/breaches when requested by the Principal (or authorised delegate).

4.3 Risk and Compliance Advisor

The Risk and Compliance Advisor is responsible for investigating complaints/breaches when requested by the Principal (or authorised delegate).

5 Review and Monitoring

This policy shall be reviewed every three years, or in the event of any information, incident, legislative changes or organisational practice that would demonstrate the need for a review.

6 Definitions

Privacy complaint: a complaint by an individual about an act or practice of the School, in relation to the individual's personal information, as defined in the *Privacy Act 1988*.

Personal information: any information that can identify a person or that can reasonably enable their identification. This information could include information such as their name, postal or email address, date of birth or financial details.

Sensitive information: information about an individual's ethnic origin, membership of political associations, philosophical beliefs, criminal record or health information.

7 Related Documents

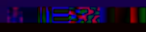
7.1 Relevant Legislation

Privacy Act 1988

Child Protection Act 1999 (Qld)

7.2 Relevant School Policies

Code of Conduct



Access to personal information is to be restricted to those persons who have a legitimate need to know the information. Appropriate arrangements should be put in place at management level to ensure that access to computerised records is granted only to staff requiring such access in the course of their duties. Where a staff member leaves the School or no longer requires access to particular records, their access to those records should be immediately terminated.

Staff members are to take reasonable precautions to ensure that personal information obtained during the course of their duties is not disclosed, either deliberately or inadvertently, to persons who do not have a legitimate need to know the information. Paper-based records should not be left where they may be accessed by unauthorised persons.

Records containing personal information should be filed securely in appropriately classified files.

5 Use of personal information

The School uses personal information concerning staff, students and third parties in conducting its business activities. Only that personal information which is relevant to the proposed activity or function will be used. Before using the information, reasonable steps will be taken to ensure that the information is up-to-date, accurate and complete.

Subject to the Privacy Act, personal information about an individual collected for a particular purpose is not to be used for another purpose. The exceptions are where:

- (a) the individual consents to the information being used for the other purpose
- (b) the proposed use is necessary to prevent or lessen a serious threat to life, health, safety or welfare of the individual or the public generally
- (c) the proposed use is authorised or required by law
- (d) the proposed use is necessary for the enforcement of the law
- (e) the purpose for which the information is to be used is directly related to the original purpose for which the information was collected
- (f) the proposed use is necessary for research in the public interest (the information is to be deidentified before publication) and it is not

practicable to seek the consent of the individual concerned.

Where information is used for a purpose for which it was not collected, a notation is to be made on the relevant record of this use.

5.1 Students and Parents/Guardians

In relation to personal information of students and

9 Updating personal information

It is important that personal information the School collects is accurate, complete and up-to-date. During the course of our relationship with members of the School community, they will be asked to keep the School informed of any changes to personal information. They can contact the School at any time to update 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 we may use or disclose it, unless we are required by or under an Australian law or a court order to retain it.

10 Checking of personal information

Under the Privacy Act, an individual has the right to obtain access to any personal information that the School holds about them and to advise the School of any perceived inaccuracy. There are some exceptions to this right set out in the Act. Students will generally have access to their personal information through their parents, but older students (over 18 years of age) may seek access themselves.

All requests to access any information the School holds must be made to the Principal in writing.

The School may be required to verify an individual's identity and specify what information they require. The School may charge a fee to cover the cost of verifying the application, locating, retrieving, reviewing and copying any material requested. If the information sought is extensive, the School will advise the likely cost in advance.

The School will seek to handle all requests for access to personal information as quickly as possible.

11 Privacy Complaints

If an individual believes that their privacy has been breached, a complaint may be made in writing to the School in the following ways:

- (a) Telephone: 07 3332 1300
- (b) Writing: Gregory Terrace, Brisbane Qld 4000
- (c) Email: admin@bggs.qld.edu.au
- (d) Facsimile: 07 3832 6097

In order to enable such a complaint to be properly investigated, it should identify the person whose privacy appears to have been breached. An investigation will be conducted in consultation with the relevant Head of Faculty/Department and the School will respond in writing.

If the complaint is not resolved to the individual's satisfaction, and more than 45 business days have passed since the complaint was made to the School, the individual may lodge a complaint with the Office of the Information Commissioner. If the person lodging the complaint as

report all eligible data breaches to the Office of the Australian Information Commissioner (OAIC).

An eligible data breach will occur if:

- (a) there is unauthorised access to, unauthorised disclosure of, or loss of, personal information held by the School
- (b) a reasonable person would conclude that the access, disclosure or loss would be likely to result in serious harm to any of the individuals to whom the information relates.

If the School has reasonable grounds to believe that a data breach has occurred in these circumstances, it must notify the OAIC and the affected individuals of the breach.

The Uej qqm'Data Breach Response Plan outlines the steps that must be followed if a data breach occurs or is suspected to have occurred.