Privacy Policy

1 Purpose

The *Information Privacy Act 2009* (Qld) (**Information Privacy Act**) and the *Federal Privacy Act 1988* (**Privacy Act**) regulate how the School collects, stores, provides access to, uses and discloses personal information. This Privacy Policy (**the Policy**) outlines the process for dealing with personal information in accordance with both State and Federal Acts.

2 Scope

This Policy applies to all board members, staff, students, parents/guardians, contractors, volunteers and visitors to the School.

3 Policy Statement

The School is committed to protecting your privacy in accordance with the Australian Privacy Principles (**APP**) contained in the Privacy Act and, as such, this Policy outlines how the School uses and manages personal information provided to or collected by the School.

This policy is based on the following principles:

(a) the School supports responsible and transparent handling of personal information

(b) the School respects an individual's right to know how their personal information will be collected, used, disclosed, stored and disposed of

(c) adequate privacy protection is a necessary condition for the School to participate in e-communications and e-transactions.

Personal information will be collected, stored, used and disclosed in accordance with the procedures outlined in **Appendix A**.

4 Roles and Responsibilities

4.1 Principal (or authorised delegate)

The Principal (or authorised delegate) is responsible for:

(a) ensuring implementation of this Policy and communication to staff, parents, students and the wider community

(b) ensuring all privacy complaints and breaches are addressed in a timely manner

(c) initiating and authorising investigations into privacy complaints and breaches, if necessary.

4.2 Chief Financial Officer (CFO)

The CFO is responsible for:

(a) ensuring management of requests for information in line with the Privacy Act and this Policy

(b) ensuring information is securely stored and a register of complaints and concerns is maintained, kept confidential and only shared with relevant parties

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

4.3 Risk and Compliance Officer

The Risk and Compliance Officer 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, that is a breach of the School's obligations under the *Information Privacy Act 2009* (Qld) and/or *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 a person's religious and political beliefs, sexual preferences, racial or ethnic origin, membership of political associations, philosophical beliefs, criminal record or health information.

7 Related Documents

The School's Code of Conduct

Information Privacy Act 2009 (Qld)

Privacy Act 1988

Child Protection Act 1999 (Qld)

Appendix A: Procedures

These procedures set out how the School intends to comply with its obligations under the Information Privacy Act 2009 (Qld) and the Privacy Act 1988.

1 Type of information collected

The type of information the School collects and holds information about:

(a) students and parents and/or guardians before, during and after the course of a student's enrolment at the School

(b) job applicants, staff members, volunteers and contractors

(c) other people who come into contact with the School.

The School will generally collect personal information about an individual by way of forms filled out in person, online via email or the website, and telephone calls. In some circumstances, the School may be provided with personal information about an individual from a third party—for example, a medical report or school reference.

2 Collection of personal information

The School collects personal information from individuals and third parties to discharge its functions, including teaching and research, and student and staff administration.

Only personal information that is necessary for a lawful function or activity of the School is to be collected.

Personal information is to be collected in a way which is lawful, fair and not unreasonably intrusive to the privacy of the individual concerned. When collecting the information, the School will take reasonable steps to ensure that the information is up-to-date, accurate and complete.

Where it is reasonable and practicable to do so, personal information is to be collected directly from the individual concerned rather than from a third party. This ensures that the information will be up-to-date and accurate, and the person to whom the information relates is aware of the collection.

When collecting information from the individual, the School will take reasonable steps to inform the person:

(a) why the information is being collected and how it is intended to be used

(b) the School's authority to collect the information

(c) any third parties to whom the School routinely gives the kind of information requested.

If a person decides not to provide requested information, it may not be possible for the School to provide the person with the services. In this circumstance, the person may be informed of the consequences of the information not being provided.

3 Exception in relation to employee records

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

4 Security of personal information

Personal information in the possession or under the control of the School will be held securely, and will be protected from unauthorised access, use, modification and disclosure by such security mechanism as are appropriate in the circumstances.

In determining the most appropriate security mechanisms, regard will be given to the following considerations:

(a) the sensitivity of the information

(b) the vulnerability of the information to misuse

(c) the form of the information (e.g. hardcopy, electronic, photographic images)

(d) the possible consequences for the person to whom the information relates of misuse of the information

(e) the availability of processes and mechanisms within the School for the protection of the information.

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 Information 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 parents/guardians, the School's primary purpose of collection is to enable the School to provide education for the student. This includes satisfying the needs of both parents/guardians and students throughout the application period and the whole period the student is enrolled at the School.

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

(a) correspondence with parents/guardians to keep parents/guardians informed about matters related to their child's schooling (including student's progress reports)

(b) publication of School newsletters, magazines and articles on the website

(c) day-to-day administration

(d) looking after students' educational, social and medical wellbeing (including disclosing student's personal information and health information to medical practitioners in an emergency)

(e) to request any previous school the student attended provide confirmation that all fees associated with the student's schooling have been paid in full

(f) the collection of debts owed to the School

(g) seeking donations and other fundraising activities for the School.

The School may publish the contact details of parents/guardians in a class list and School directory. If parents do not consent to their contact details being published in a class list and/or School directory, they must notify the School.

5.2 Job applicants, staff members and contractors

In relation to personal information of job applicants, staff members and contractors, the School's primary purpose of collection is to assess and (if successful) to employ the applicant, staff member or contractor, as the case may be.

The purposes for which the School uses personal information of job applicants, staff members and contractors include:

(a) in administering the individual's employment or contract, as the case may be

(b) for insurance purposes

(c) seeking funds and marketing the School

(d) to satisfy the School's legal requirements.

5.3 Volunteers

The School also obtains personal information about volunteers who assist the School in its functions or associated activities, such as alumnae associations and parent/guardian support groups to enable the School and the volunteers to work together.

5.4 Marketing and Fundraising

The School treats marketing and seeking donations for the future growth and development of the School as an important part of ensuring the School continues to be a quality learning environment.

Personal information held by the School may be disclosed to an organisation that assists in the School's fundraising and marketing, for example, the School's alumnae organisation.

Parents, staff, contractors and other members of the wider School community may, from time-to-time, receive fundraising information and school publications, like newsletters and magazines.

If they do not wish to receive any such information, they should advise the School via: phone on 07 3332 1300 or by email to communications@bggs.qld.edu.au.

Upon receiving communication that they do not wish to receive this information, the School will stop sending such information. They will however continue to receive official School communication.

6 Anonymity and consequences of not providing personal information

If it is lawful and practicable to do so, the School may offer the opportunity of dealing with us anonymously or by using a pseudonym. For example, when making a general inquiry about the School.

However, it is not possible for the School to enrol or continue the enrolment of a student or provide education for the student if the student or her parents/guardians wish to interact anonymously or using a pseudonym.

7 Disclosure of personal information

The School may disclose personal information, possibly including sensitive information, held about an individual to:

(a) another school

(b) government departments

(c) medical practitioners

(d) people providing services to the School, including specialist visiting teachers and sports coaches

(e) recipients of school publications, like newsletters and magazines

(f) parents

(g) anyone to whom you authorise the School to disclose information.

8 Disclosure of information overseas

The school may disclose personal information about an individual to overseas recipients, for instance, to facilitate a school exchange. However, the School will not send personal information about an individual outside Australia without:

(a) obtaining the consent of the individual (in some cases this consent will be implied)

(b) otherwise complying with the Australian Privacy Principles (APP) or other applicable privacy legislation.

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 (as detailed in Appendix A), 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 the persons' 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 topersonal 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 any queries about how to do so, they can contact the Office of the Australian Information Commissioner by telephoning 1300 363 992.

12 Changes to this Privacy Policy

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

If the School changes its Privacy Policy, it will place an updated version on the website: www.bggs.qld.edu.au.

13 Privacy breaches

All staff are responsible for reporting any breaches of this Policy to the Head of their Faculty or Department, or to a member of the Executive Management team, as soon as practicable after the breach has been identified. Following notification, management will:

(a) for minor breaches of the Policy: liaise with the relevant Head of Faculty or Department on the necessary actions required to prevent a similar breach from occurring

(b) for major breaches of the Policy: instigate an investigation into the breach.

The Chief Financial Officer must be informed of breaches of this policy or procedure and any actions arising out of any investigations.

A breach of this Policy or procedure may, depending on the circumstances, constitute a breach of the School's Code of Conduct.

14 Notifiable Data Breach scheme

In adherence with the Privacy Act 1988, under the Notifiable Data Breach scheme, it is mandatory for the School to 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 Data Breach Response Plan (Appendix B) outlines the steps that must be followed if a data breach occurs or is suspected to have occurred.

BRISBANE GIRLS GRAMMAR SCHOOL

Appendix B: Data Breach Response Plan

This data breach response plan (**response plan**) sets out procedures and clear lines of authority for Brisbane Girls Grammar School staff in the event that the School experiences a data breach (or suspects that a data breach has occurred).

A data breach (Appendix A) occurs when personal information is lost or subjected to unauthorised access, modification, use or disclosure, or other misuse that is likely to cause serious harm. Data breaches can be caused or exacerbated by a variety of factors, affect different types of personal information and give rise to a range of actual or potential harm to individuals, agencies and organisations.

This 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. It sets out contact details for the appropriate staff in the event of a data breach, clarifies the roles and responsibilities of staff, and documents processes to assist Girls Grammar to respond to a data breach.

The School experiences data breach/data breach suspected

Discovered by staff member, or the School otherwise alerted

<u>What should the staff member do?</u>

Immediately notify your Director/Manager of the suspected data breach

Record and advise them of the time and date the suspected breach was discovered, the type of personal information that was involved, the cause and extent of the breach, and the context of the affected information and the breach

<u>What should the Director / Manager do?</u>

Determine whether a data breach has or may have occurred

Determine whether the data breach is serious enough to escalate to the Data Breach Response Team Coordinator (CFO) (some breaches may be able to be dealt with at the Director/Manager level)

If so, immediately escalate to the Data Breach Response Team Coordinator

Alert the School Data Breach Response Team Coordinator (CFO)

Coordinator convenes Data Breach Response Team

Corporate and Communications	**Primary contact** Director of C&E **Secondary contact** PA to the Principal	Legal and Records	**Primary contact** CFO **Secondary contact** Deputy Principal	IT	**Primary contact** Director of IT **Secondary contact** IT Manager	Breach Assessment and Regulations	**Primary contact** Director of HR **Secondary contact** Risk & Compliance Officer

1 When should Directors/Managers escalate a data breach to the School Data Breach Response Team?

1.1 Directors/Managers to use discretion in deciding whether to escalate to the response team

All staff should report a suspected data breach to their Director/Manager.

Some data breaches may be comparatively minor, and able to be dealt with easily without action from the Data Breach Response Team (response team).

Directors/Managers should use their discretion in determining whether a data breach or suspected data breach requires escalation to the response team. In making that determination, they should consider the following questions:

(a) Are multiple individuals affected by the breach or suspected breach?

(b) Is there (or may there be) a real risk of serious harm to the affected individual(s)?

(c) Does the breach or suspected breach indicate a systemic problem in the School's processes or procedures?

(d) Could there be media or stakeholder attention as a result of the breach or suspected breach?

If the answer to any of these questions is 'yes', then the Director/Manager should notify the response team.

The School has an obligation to notify individuals whose personal information is involved in a data breach that is likely to result in *serious harm*. This notification must include recommendations about the steps individuals should take in response to the breach. The Australian Information Commissioner (Commissioner) must also be notified of eligible data breaches.

The notification to affected individuals and the Commissioner must include the following information:

(a) the identity and contact details of the organisation

(b) a description of the data breach

(c) the kinds of information concerned

(d) recommendations about the steps individuals should take in response to the data breach.

1.2 Director/Manager to inform the response team Coordinator (CFO) of minor breaches

If a Director/Manager decides not to escalate a minor data breach or suspected data breach to the response team for further action, the Director/Manager should:

(a) **send a brief email to the response team Coordinator** (CFO) that contains the following information:

- description of the breach or suspected breach
- action taken by the Director/Manager or staff member to address the breach or suspected breach
- the outcome of that action
- the Director/Manager's view that no further action is required.

(b) **save of copy of that email in to T drive (T:\Senior Management)**:

- Data Breach Response—reports and investigation of data breaches within the School's network drive.

2 BGGS Data Breach Response Team checklist

2.1 Process

There is no single method of responding to a data breach. Data breaches must be dealt with on a case-by-case basis, by undertaking an assessment of the risks involved, and using that risk assessment to determine the appropriate course of action.

There are four key steps to consider when responding to a breach or suspected breach.

(a) **STEP 1**: **Contain the breach and do a preliminary assessment**

(b) **STEP 2: Evaluate the risks associated with the breach**

(c) **STEP 3**: **Notification**

(d) **STEP 4**: **Prevent future breaches**

The data breach should immediately be contained and, if necessary, IT will implement the School's Incident Response Plan.

The response team should ideally undertake steps 1, 2 and 3 either simultaneously or in quick succession.

The response team should refer to the Australian Government OAIC's *Data breach notification: a guide to handling personal information security breaches* (https://www.oaic.gov.au/agencies-and-organisations/guides/data-breach-notification-a-guide-to-handling-personal-information-security-breaches), which provides further detail on each step.

Depending on the breach, not all steps may be necessary, or some steps may be combined. In some cases, it may be appropriate to take additional steps that are specific to the nature of the breach.

In reconsidering processes and procedures to reduce the risk of future breaches (Step 4), the response team should also refer to the Australian Government OAIC's *Guide to securing personal information* (https://www.oaic.gov.au/agencies-and-organisations/guides/guide-to-securing-personal-information). This guide presents a set of non-exhaustive steps and strategies that may be reasonable for the School to take in order to secure personal information, and considers actions that may be appropriate to help prevent further breaches following an investigation.

The following checklist is intended to guide the response team in the event of a data breach, and alert the response team to a range of considerations when responding to a data breach.

2.2 Records management

Documents created by the response team should be saved in T Drive (T:\Senior Management).

Step 1 **Contain the breach and make a preliminary assessment**	□	Convene a meeting of the Data Breach Response Team.
	□	Immediately contain breach: □ IT to implement an *Incident Response Plan* if necessary.
	□	Inform the School's Executive and provide ongoing updates on key developments.
	□	Ensure evidence is preserved that may be valuable in determining the cause of the breach, or allowing BGGS to take appropriate corrective action.
	□	Consider developing a communications or media strategy to manage public expectations and media interest.
Step 2 **Evaluate the risks for individuals associated with the breach**	□	Conduct initial investigation, and collect information about the breach promptly, including: □ the date, time, duration and location of the breach □ the type of personal information involved in the breach □ how the breach was discovered and by whom □ the cause and extent of the breach □ a list of the affected individuals, or possible affected individuals □ the risk of serious harm to the affected individuals □ the risk of other harms.
	□	Determine whether the context of the information is important.
	□	Establish the cause and extent of the breach.
	□	Assess priorities and risks based on what is known.
	□	Keep appropriate records of the suspected breach and actions of the response team, including the steps taken to rectify the situation and the decisions made.
Step 3 **Consider breach notification**	□	Determine who needs to be made aware of the breach (internally, and potentially externally) at this preliminary stage.
	□	Determine whether to notify affected individuals—is there a real risk of serious harm to the affected individuals? In some cases, it may be appropriate to notify the affected individuals immediately, for example, where there is a high level of risk of serious harm to affected individuals.
	□	Notify the Australian Information Commissioner (Commissioner) if a data breach is likely to result in serious harm.
	□	Consider whether others should be notified, including police/law enforcement, or other schools or organisations affected by the breach, or where the School is contractually required or required under the terms of an MOU or similar obligation to notify specific parties.
Step 4 **Review the incident and take action to prevent future breaches**	□	Fully investigate the cause of the breach.
	□	Report to the School's Executive on outcomes and recommendations: □ Update security and response plan if necessary □ Make appropriate changes to policies and procedures if necessary □ Revise staff training practices if necessary □ Consider the option of an audit to ensure necessary outcomes are effected

3 How do data breaches occur?

Data breaches occur in a number of ways. Some examples include:

(a) lost or stolen laptops, removable storage devices, or paper records containing personal information

(b) hard disk drives and other digital storage media (integrated in other devices, for example, multifunction printers, or otherwise) being disposed of or returned to equipment lessors without the contents first being erased

(c) databases containing personal information being 'hacked' into or otherwise illegally accessed by individuals outside of the organisation

(d) employees accessing or disclosing personal information outside the requirements or authorisation of their employment

(e) paper records stolen from insecure recycling or garbage bins

(f) mistakenly providing personal information to the wrong person, for example by sending details out to the wrong address

(g) an individual deceiving the School or an employee into improperly releasing the personal information of another person.