RISK MANAGEMENT POLICY AND COMPLIANCE FRAMEWORK

This policy confirms the commitment of the Board of Directors to good corporate governance through risk management and compliance. It defines the broad accountabilities and structures the School will maintain in order to manage risk and compliance.

Risk arises in all aspects of the School’s operations and at all stages within the life cycle of those operations. It offers both opportunity and threat, and must therefore be managed appropriately. The School is committed to adopting a strategic, consistent and structured enterprise-wide approach to risk management in order to achieve an appropriate balance between realising opportunities for gains and minimising losses.

Risk and Compliance Definitions have been identified in Appendix A.

1. Purpose of Policy
a) The Board of Directors and Management of the School are committed to the implementation and maintenance of a formal risk management system, including the integration of risk management throughout all levels of the School as fundamental to achieving the School’s strategic and operational objectives. This policy outlines the framework that reflects that commitment. The School’s Risk Management Framework is based on the Australia/New Zealand Risk Management Standard AS/NZS 4360:2007.

b) The School is committed to delivering its strategic and operational objectives in accordance with the principles of good governance, in compliance with a diverse range of state and commonwealth legislation; statutory and regulatory requirements, and reporting obligations whilst reducing its risk to acceptable levels with the implementation of risk treatments that includes internal policies and procedures. This policy therefore also aims to assist the School to meet those legal and statutory obligations and determine compliance with School policies and risk treatments as documented in the risk registers. The Compliance Policy conforms to the Australian Standard AS 3806 – 1998 Compliance Programme.

2. Application of Policy
a) This policy applies to the School Board of Directors and its Committees, staff, and members of Support Groups.

3. Risk Management Policy Statement
a) In its application of this policy, the School is committed to:
   - Achieving its strategic and operational objectives while minimising the impact of significant risks that the School can meaningfully and realistically control;
   - Protecting and enhancing the School’s reputation;
   - Behaving as a responsible and ethical corporate citizen, protecting staff, students and the broader community from harm and protecting physical property from loss or damage;
   - Establishing the right balance between the cost of control and the risks it is willing to accept as part of the business and industry environment within which it operates;
   - Recognition and exploitation of opportunities;
b) Risk Appetite

- Risk appetite is the amount of risk, on a broad level, that the School is willing to accept in pursuit of value, and should reflect:
  - risk management philosophy per location, project, process, etc.
  - capacity to take on risk.
  - School objectives, business plans and respective stakeholder demands.
  - evolving industry and market conditions.
  - tolerance for failures with quantitative values, where applicable.
- The School’s risk appetite will be reassessed by the Board on a regular basis. The School’s risk appetite will be recorded on individual risk registers as residual risk ratings accepted and reported to the Board in the monthly Board report.
- It is acknowledged that the School must at times undertake activities that carry significant risks.

4. Compliance Policy Statement

The School is committed to the maintenance and continuous improvement of a compliance programme, and to the development of a compliance culture throughout the School.

The Compliance Programme is an approach to monitoring and addressing the:

- risk profile and responsibilities as identified in the Risk Management Framework; and
- legal, regulatory and other obligations that govern the operations of the School.

The School will allocate appropriate resources to the development, implementation and continuous improvement of its compliance programme.

The School will adopt a risk-based approach to the implementation of its compliance programme. Statutory obligations representing the greatest degree of risk to the School will be given priority. Compliance responsibilities will be allocated to the risk owners as identified within the risk register. Behaviours that create and support compliance will be encouraged. Behaviours that compromise compliance will be investigated.

The Compliance programme will mainly consist of control self-assessment checklist create from risk treatment plans identified within the risk registers. These checklists will be completed at least annually for all key areas within the School.

A programme of external assurance will also be maintained for any critical inherent risks as identified by the Business Manager in consultation with the Board. These reviews will be scheduled in a three year cycle.

The Business Manager will report monthly to Board of Directors and quarterly to the Finance Committee on the School’s compliance programme.
5. Risk and Compliance Categories
Risks will be identified and managed in functional areas. The key areas will be:
- Strategic Risks
- Governance and Board functions
- Human Resources
- Enrolments
- Other Stakeholders / Communications
- Students
  - Pastoral Care
- Curriculum
  - Curriculum Management and Development
  - Science
  - Health and Physical Education
- Co-curriculum
- Finance
- Information Technology
- Facilities

The risk process and corresponding risk methodology have been identified in Appendix B and C.

6. Risk Management and Compliance Responsibilities
a) Board of Directors
   - Board of Directors retains the ultimate responsibility for risk management and for determining the appropriate level of risk that the School is willing to accept.
   - Board of Directors is responsible for overseeing the School’s compliance with external legislation, statutory and regulatory requirements, reporting obligations, and School policies.

b) Finance Committee/Buildings and Grounds Committee
   - The Finance Committee will advise the Board of Directors on Risk Management and Compliance for issues relating to Finance. The Buildings and Grounds Committee will advise the Board on Risk Management and Compliance for issues relating to Facilities and Workplace Health and Safety.

c) Principal
   - The Principal is responsible for ensuring that risk management activities are carried out effectively within the School.
   - The Principal may approve policies and/or procedures relating to Business Continuity Management, Critical Incident Management and IT Disaster Recovery. The Principal may also approve any Risk Management procedures.
   - The Principal is responsible for approving the School’s Compliance Procedures and for ensuring that these are aligned with the School’s strategic and operational objectives and relevant state and federal legislation.
d) Business Manager

- The Business Manager is responsible for the development of systems, processes and procedures that promote effective Risk Management.
- The Business Manager is responsible for ensuring that risk management activities are carried out in accordance with the Risk Management Policy and Procedures.
- The Business Manager is responsible for compiling regular reports for the Board and Finance and Buildings and Grounds Committees regarding risk management and compliance issues.
- The Business Manager will have overarching responsibility for:
  - coordinating the maintenance of the Compliance programme in accordance with the policy and procedures;
  - providing support and training to staff where appropriate; and
  - monitoring and reporting on compliance.

e) Risk Owners

- A Risk Owner will be assigned for each risk area within the School, as detailed in the School Risk Register.
- A Risk Owner will generally be the most senior staff member of the School, who is responsible for the management of the particular risk.
- It is the Risk Owner’s responsibility to provide the Business Manager with information to report to the Board of Directors on progress against mitigation plans and the results of compliance reviews and risk assessments performed on new initiatives.
- Risk Owners will be accountable for the recognition and management of compliance risks in their area and for reporting on compliance.

f) All School Staff

- All staff will diligently identify risks and report them to their supervisor, especially during periods of change to processes or operational practice.
- Staff will comply with all risk treatments.
- All staff must be aware of compliance responsibilities that apply to their area of work or activities, and ensure that their actions on behalf of the School comply with relevant laws.

7. Risk Monitoring and Reporting

All inherent High - Critical risks will be reported to the Board on an annual basis together with the results of the compliance self-assessment.
All inherent High - Critical risks for Finance, Facilities and ICT will be reported to the Finance Committee on an annual basis together with the results of the compliance self-assessment.
Appendix A: Definitions

**Residual Risk** means the level of risk that remains after assessing the effectiveness of the controls, management strategies and other mechanisms currently in place to mitigate a particular risk.

**Risk** means a risk to the School that has the potential to threaten the achievement of our objectives.

**Risk Management** refers to the culture, processes and structures developed to effectively manage potential opportunities and adverse effects for any activity, function or process undertaken by the School. The process of managing risk is achieved through the systematic application of policies, procedures and practices to establish the context, identify, analyse, evaluate, treat, monitor and communicate risk.

**Risk Analysis** means a systematic use of available information to determine how often specified events may occur and the magnitude of their consequences;

**Consequence** means the outcome of an event expressed qualitatively or quantitatively, being a loss, injury, disadvantage or gain. There may be a range of possible outcomes associated with an event;

**Likelihood** means a qualitative description of probability or frequency;

**Loss** means any negative consequence, financial or otherwise;

**Risk Appetite** means the amount of risk that the School is prepared to accept or be exposed to at any point in time;

**Risk Treatment** means selection and implementation of appropriate options for dealing with risk.

Characteristics of a **Significant Incident** include, but are not limited to:

- Incident requiring management by a senior member of staff to allow appropriate, prompt decisions to be made
- Minor injuries to staff, students or other members of the general public
- Potential trauma to staff and/or students
- Potential for external media to become aware of the situation
- Impact on critical IT service availability to the School with a potential down time of up to 2 hours.

**Significant Incidents** may include:

- Staff or student injuries that may require medical attention
- Staff/student violence
- Repairable damage to buildings
- IT outage up to 2 hours; and/or
- Temporary telephone system outage.

**School Risk Register** means the register that records information about the corporate risks faced by the School and relevant controls being put in place to mitigate against them.

**Compliance** means the process of adhering to the law and the obligations and requirements arising from the law;

**Compliance culture** means the sum of values, ethics and beliefs that exist throughout an organisation and which interact with the organisation’s structures and control systems to produce behavioural norms that are conducive to compliance outcomes;

**Compliance failure** means an act or a failure to act to meet the organisation’s compliance obligations, processes or behavioural obligations;

**Compliance programme** means a series of activities designed to achieve compliance;

**Register of Compliance Obligations** is the list of compliance requirements that have been identified by the School.
Appendix B: Risk Management Procedures

The Risk Management Process

1. The School will utilise a risk management process that consists of the following key stages:
   a) Risk Identification: Identifying all reasonably foreseeable risks associated with its activities,
   b) Risk Rating: Quantifying those risks (inherent and residual) using the criteria detailed in Appendix D.
   c) Risk Controls / Treatments: Assessing the risk, identifying options to treat risks and developing mitigation plans.
   d) Risk Monitoring and Reporting: Performing self-assessment of compliance with risk treatments and reporting the results to the Board and Finance and Audit Committee in line with the Compliance Programme.

2. Risk Identification
   A key mechanism for the identification of risks at the School is the development and maintenance of the School’s Risk Register. Risks will be identified in the context of Strategic Priorities, Compliance to legislation and Health and Safety requirements.
   The Risk Register identifies the key risks that may potentially prevent the School from achieving its objectives. The register outlines the key risks, inherent risk rating, residual risk rating, and controls currently in place to manage the risk and action plans to address those risks.
   Risks may also be added to the School’s Risk Register on a periodic basis throughout the year.
   All new initiatives undertaken by the School, such as IT, capital expenditure and commercial ventures, will require a risk assessment as part of the project development phase. All School overnight School excursions will require a separate risk register.

3. Risk Rating
   Risks will be rated in accordance with the tables in Appendix D as follows:
   - Risks will be assessed and rated in terms of the potential consequence of the risk and the likelihood of the risk occurring.
   - Risks will be assessed without controls i.e. inherent risks as well as with controls i.e. residual risks.
   - All identified risks will be rated consistently using the criteria and rating scales contained in the Appendix D. The consequence rating should be assigned to a risk when considering the consequences to the School as a whole.

4. Risk Treatments / Controls
   Options for treating each risk will be identified. The options will be evaluated and accountability for the risk will be assigned. Risk treatment plans will be prepared and implemented.
   The following options may be used for treating risks and will be determined in the light of risk appetite and risk assessment:
   - Avoid the risk
   - Mitigate the risk
   - Transfer the risk; and
   - Accept the risk.
Risk mitigation, or risk treatment, involves putting in place controls to reduce the level of residual risk to a level that is considered acceptable by the School. This is also known as the target risk rating. Risk mitigation plans will be developed for all risks that are rated residually as Critical, High, or Moderate.

5. Actions
Where residual risks status is above the School’s risk appetite additional risk treatments will be identified these will be detailed as ‘Action Items’ in Risk Owner’s Reports. Action items will include due dates and will be followed up and reported on.
Appendix C: Risk Matrix

The following matrix notes the two dimensions in which all risks will be assessed. Risks Owners will be allocated in according with functional levels e.g. Facilities or Finance.

For all risks in a function where appropriate a process level will be identified e.g. Chemical spill risk will be documented in the Curriculum Functional area and will also be identified as a Health and Safety risk. This will provide the opportunity to review risks either as processes e.g. all School Health and Safety risks or Function e.g. all Facilities risks.
Appendix D: Risk Rating Scales and Tables

Likelihood Levels

Likelihood generally describes the probability or frequency of an event. The likelihood of an event can be classified as:

- **Almost Certain**: The event is generally expected to occur at least every year; except for ICT risk ratings which will be moderated based on the school’s ability to continue to function.
- **Likely**: The event is generally expected to occur at least every 3 years.
- **Possible**: The event is generally expected to occur at least every 10 years.
- **Unlikely**: The event is generally expected to occur at least every 30 years.
- **Rare**: The event is generally expected to occur no more frequently than every 40 years.

Risk Matrix

The following matrix, and the Likelihood and Consequence Levels as defined below have been adapted from the Australian/New Zealand Standard on Risk Management (AS/NZS 4360:2004).

<table>
<thead>
<tr>
<th>Likelihood</th>
<th>Almost Certain (expected at least within every year) NOTE: special arrangements for rating ICT – ratings will be moderated based on the school’s ability to continue to function.</th>
<th>Highly Likely (expected at least every 3 years)</th>
<th>Reasonably Likely (expected at least every 10 years)</th>
<th>Low Likelihood (expected at least every 30 years)</th>
<th>Rare (expected, if at all, not more frequently than every 40 years)</th>
</tr>
</thead>
<tbody>
<tr>
<td>CONSEQUENCE</td>
<td>Trivial</td>
<td>Minor</td>
<td>Moderate</td>
<td>Substantial</td>
<td>Extreme</td>
</tr>
<tr>
<td>L</td>
<td>M</td>
<td>H</td>
<td>C</td>
<td>C</td>
<td></td>
</tr>
<tr>
<td>L</td>
<td>M</td>
<td>H</td>
<td>C</td>
<td>C</td>
<td></td>
</tr>
<tr>
<td>L</td>
<td>M</td>
<td>M</td>
<td>H</td>
<td>C</td>
<td></td>
</tr>
<tr>
<td>L</td>
<td>L</td>
<td>M</td>
<td>M</td>
<td>H</td>
<td></td>
</tr>
<tr>
<td>L</td>
<td>L</td>
<td>M</td>
<td>M</td>
<td>H</td>
<td></td>
</tr>
</tbody>
</table>

The consequence will be assessed using the table below.
## Risk Consequence Summary

<table>
<thead>
<tr>
<th>RISK RATING</th>
<th>TRIVIAL</th>
<th>MINOR</th>
<th>MODERATE</th>
<th>SUBSTANTIAL</th>
<th>EXTREME</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Damage to Reputation</strong></td>
<td>Minor negative publicity</td>
<td>Adverse contained publicity</td>
<td>Significant adverse publicity in public domain</td>
<td>Sustained adverse publicity state-wide. Ministerial dissatisfaction</td>
<td>Loss of accreditation, Action required by Minister</td>
</tr>
<tr>
<td><strong>Health &amp; Welfare of Students &amp; Staff</strong></td>
<td>Minor injury not requiring first aid treatment</td>
<td>Minor injury requiring first aid treatment</td>
<td>Hospitalisation required for injury/s, but full recovery anticipated</td>
<td>Serious medical condition/injury's requiring hospitalisation and long term care</td>
<td>Very significant risk of extensive injuries requiring extended hospitalisation and or serious permanent damage / Death</td>
</tr>
<tr>
<td><strong>Year 12 Results</strong></td>
<td>Minimal change to the distribution of OP scores year on year</td>
<td>25% reduction in the number of OP1 and OP2 scores year on year</td>
<td>25% reduction in the number of OP1 and OP2 scores year on year accompanied by reduction in overall results</td>
<td>25-50% reduction in the number of OP1 and OP2 scores year on year accompanied by significant reduction in the number of tertiary placements</td>
<td>&gt;50% reduction in the number of OP1 and OP2 scores year on year accompanied by significant reduction in the number of tertiary placements</td>
</tr>
<tr>
<td><strong>Financial</strong></td>
<td>&lt; $5,000</td>
<td>$5,000 - $50,000</td>
<td>$50,001 - $500,000</td>
<td>$500,001 - $1,000,000</td>
<td>&gt; $1,000,000</td>
</tr>
<tr>
<td><strong>Breach of Legislation</strong></td>
<td>Minor administrative breach, rectified after identification</td>
<td>Minor breach resulting in caution and corrective action</td>
<td>Breach resulting in fine or corrective action</td>
<td>Major breach resulting in fines and damages</td>
<td>Severe breach resulting in substantial litigation</td>
</tr>
<tr>
<td><strong>Reduction in Enrolments</strong></td>
<td>Minor reduction in enrolments (&lt;5 students)</td>
<td>Reduction of 5 – 10 students</td>
<td>Reduction of 10 – 25 students</td>
<td>Reduction of 25 – 75 enrolments</td>
<td>Reduction &gt; 75 students</td>
</tr>
<tr>
<td>RISK RATING</td>
<td>TRIVIAL</td>
<td>MINOR</td>
<td>MODERATE</td>
<td>SUBSTANTIAL</td>
<td>EXTREME</td>
</tr>
<tr>
<td>--------------------------</td>
<td>----------------------------------------------</td>
<td>--------------------------------------------</td>
<td>--------------------------------------------</td>
<td>----------------------------------------------</td>
<td>----------------------------------------------</td>
</tr>
<tr>
<td><strong>Security</strong></td>
<td>Localised incident. Minor or no effect on operations</td>
<td>Localised incident. Moderate effect on operations fixed within 2 hours</td>
<td>Significant incident. Sustained effect on operations less than 1 day effect on business.</td>
<td>Severe incident resulting in total shutdown and/or loss of data 1-2 day’s system outage.</td>
<td>Long term impact to ongoing service delivery and or regulatory ‘fall-out’ due to delayed recovery of data / permanent loss of data. Or outage exceeding 2 days.</td>
</tr>
<tr>
<td><strong>Loss of Quality Staff</strong></td>
<td>Routine resignations due to personal circumstances only</td>
<td>Routine resignations and leave situations resulting in &lt; 10% change</td>
<td>Inability to replace a staff member/s in adequate time. Resignation 11-15% change</td>
<td>&gt;15% but &lt; 30% resignations owing to dissatisfaction with organisation and/or inability to appoint replacements</td>
<td>&gt;30% resignations owing to dissatisfaction with organisation and inability to appoint replacements</td>
</tr>
<tr>
<td><strong>Disruption to Curriculum/Operations</strong></td>
<td>Timetabling issues but no interruption to classes</td>
<td>Disruption to some classes but manageable by altered programme</td>
<td>Disruption to a number of classes over a period of time</td>
<td>All classes affected over a sustained period of time</td>
<td>Total dysfunction and total shutdown of classes</td>
</tr>
<tr>
<td><strong>Disruptions to ICT Systems</strong></td>
<td>Inconvenience but no interruption to classes/operations</td>
<td>Disruption to some classes/ departments but manageable by altered programme</td>
<td>Disruption to a number of classes/ department s over a period of time</td>
<td>All classes/ departments affected over a period of time</td>
<td>Total dysfunction and total shutdown for more than a week</td>
</tr>
</tbody>
</table>
Assessing Residual Risks

The Risk Register includes an assessment of both the identified ‘inherent’ risks (i.e. the risk before evaluation of the effectiveness of relevant controls) and the ‘residual’ risk (after such evaluation) the School staff are therefore required to assess the effectiveness of the controls in place using an effectiveness rating.

<table>
<thead>
<tr>
<th>Effectiveness of Controls</th>
<th>Descriptor</th>
</tr>
</thead>
<tbody>
<tr>
<td>Very effective</td>
<td>The control achieves its intended outcome and is fully implemented</td>
</tr>
<tr>
<td>Partially Effective</td>
<td>The control only partially achieves its intended outcome or is not yet fully implemented</td>
</tr>
<tr>
<td>Ineffective</td>
<td>The control does not achieve its intended outcome or is not yet fully implemented</td>
</tr>
</tbody>
</table>

TAS acknowledges the work of Brisbane Girls Grammar School in compiling this Policy Framework.