ROCKHAMPTON GIRLS GRAMMAR SCHOOL

Information Security Policy

PURPOSE OF THE POLICY

This policy concerns the confidentiality of computer records at Rockhampton Girls Grammar School and the School's response to security of computer data and records generally. This policy is based on the draft Australian Standard on Information Security Management.

POLICY

Policy Statement:

The management and staff of Rockhampton Girls Grammar School support information security and confidentiality in relation to records of staff, students, parents and members of the Board of Trustees. These records will be made available under appropriate conditions as determined by the Principal.

Compliance with legislative and statutory requirements

- The School will at all times comply with legal or statutory requirements regarding security and access to records.
- Software copying will be in accordance with legal requirements, and 'pirate' software is not permitted on any School-owned computer.
- The privacy of staff, student and family records will be maintained through restricted access to records by relevant staff responsible for maintaining same.

Security education of staff and staff responsibility for information security

- Staff will be made aware through this policy and other appropriate forums (e.g. staff meetings), of the need to maintain information security.
- Staff members are required to maintain confidentiality with reference to student and family records and information, as outlined in privacy legislation.
- This policy and the School's privacy policy will be included in the staff handbook.

Access to School records by external third parties

- Access to student, staff and family records will be given only on the authorisation of the Principal or her delegate where required by law or statutory authority.
- Third parties will not be given unsupervised access to School records.
- Confidential documents or records are not to be left on desktops to be viewed by third parties, after hours staff etc.

Reporting suspected security breach incidents

- Any known security breaches identified by staff should be reported to their immediate supervisor as soon as possible. Staff members are to also report suspected security weaknesses and software malfunctions.
- A formal discipline process will be entered into for staff involved in security breaches under the direction and supervision of the Principal. This process may involve official warning, counselling or termination of a staff member's employment according to the severity of the breach.

POLICY RELEASE DETAILS

Date of Policy	September 2011
Reviewed by	RGGS Executive
Review Date	Biennially
Access	Public Availability – RGGS Website

RELATED POLICIES AND DOCUMENTS

RGGS Privacy Policy
RGGS Acceptable Use Policy
RGGS Electronic Communications Policy