RAMBERT SCHOOL
IT POLICY – SECURITY

1.1 Background

This IT Security Policy is based upon the International Standard ISO 17799 (BS 7799) The Code of Practice for Information Security Management, which is the de facto standard for the development of information security strategy world-wide.

1.2 Requirements for Policy

Rambert School has an obligation to its staff and students to clearly define requirements for the use of its information technology (IT) facilities and its information systems (IS). This is so that users of IT/IS facilities do not unintentionally place themselves, or Rambert, at risk of prosecution, by carrying out computer related activities outside the law.

1.3 Policy Structure

This document forms Rambert's Information Security Policy (henceforth referred to as The Policy). Its purpose is to provide an overarching framework (a commitment of undertaking) to apply information security controls throughout the School.

1.4 Purpose and Scope

Information plays a major role in supporting the school's academic and administrative activities. The purpose of The Policy is to provide a framework for protecting:

- Rambert's IT/IS infrastructure;
- key data and information;
- those who have access to or who administer IT/IS facilities;
- individual's who process or handle key data and information.

The Policy is designed to provide protection from internal and external security threats, whether deliberate or accidental by:

- defining Rambert's policy for the protection of the Confidentiality, Integrity and Availability of its' key data and information;
- establishing responsibilities for information security;

1.5 Objective

- *Confidentiality* - knowing that key data and information can be accessed only by those authorised to do so;
- *Integrity* - knowing that key data and information is accurate and up-to-date, and has not been deliberately or inadvertently modified from a previously approved version; and,

- *Availability* - knowing that the key data and information can always be accessed.

Rambert is committed to protect both its members and its key data and information and to deploy controls that minimise the impact of any Security Incidents.

1.6 Applicability

The Policy applies to the following categories, referred to hereafter as '*subjects*'.

- all full-time, part-time and temporary staff employed by, or working for or on behalf of Rambert;
- students studying at Rambert;
- contractors and consultants working for or on behalf of Rambert;
- all other individuals and groups who have been granted access to the school's IS/IT systems and/or key data and information.

The Principal is ultimately responsible for ensuring that The Policy is implemented and it is the personal responsibility of each person to whom The Policy applies to adhere with its requirements.

Organisational Security

2.1 Ownership and Maintenance of the Policy

The policy will be updated and reviewed by the Head of Administration, who will report to the Principal of Rambert School.

2.2 Security of Third Party Access

Access to Rambert's information processing facilities by third parties will only be permitted to the subcontracted IT Support Provider. In agreeing to a contract of employment, the IT Provider will agree to adhere to the terms of this policy and it's related documentation.

3 Assets

3.1 Inventories of information assets, including hardware, software will be maintained by the designated staff member and overseen by the Head of Administration

4 Personnel security

Controls will be deployed to reduce the risks of human error, theft, fraud, nuisance or malicious misuse of facilities.

4.1 Security in Job Descriptions

Job Descriptions will include specific responsibilities for the protection of particular assets, or the execution of particular processes or activities such as data protection.

4.2 Personnel Screening Policy

Steps will be taken to minimise the likelihood of personnel, who pose a security risk, being employed in posts involving key data and information, such as those concerned with financial or personnel related data. This will usually be determined through the appointment process, including references and through an enhanced CRB Check.

4.2.1 Confidentiality Undertaking

All members of staff are reminded of their obligation to protect confidential information in accordance with Rambert's standard terms and conditions of employment.

4.3 Reporting Security Incidents

All actual and suspected security incidents are to be reported in accordance with the Security Incident & Computer Misuse Policy in Appendix B of this document.

4.3.2 Removal and Reinstatement of Internet Access

Computers that are implicated in security incidents network will have Internet access removed in accordance with the Security Incident & Computer Misuse Policy. Subsequent reinstatement of Internet access will only be permitted when remedial action has been taken in accordance with that policy.

4.3.3 Network Isolation and Reconnection

Any computer that is perceived to be placing the integrity of the school network at risk will be disconnected at the network. Subsequent reinstatement will only be permitted once the security of the computer has been established and agreed by the external IT support provider and the Head of Administration.

4.3.4 Security Incident Management

Events that are regarded as being 'security incidents' will be defined, and processes implemented to investigate, control, manage and review such events in accordance with the Security Incident & Computer Misuse Policy, with a view to preventing recurrence. It will be the responsibility of the External IT support provider to keep Rambert informed of any security breach and subsequent action to resolve the issues.

5. Physical and environmental security

Controls will be implemented as appropriate to prevent unauthorised access to, interference with, or damage to, information assets.

5.1 Physical Security

Computer systems and networks will be protected by suitable physical and technical security controls

File servers and machines that hold or process high criticality, high sensitivity or high availability data will be located in physically secured areas.

Access to facilities that hold or process high criticality, high sensitivity or high availability data will be controlled. Laptop computers and remote equipment will be protected in accordance with the Mobile & Remote Working Policy as detailed in Appendix C

6. Communications and operations management

6.1 Documented Operating Procedures

Sensitive documentation will be held securely and access restricted to staff on a need to know basis.

6.2 Segregation of Duties

Access to critical systems and key data and information will only be granted on a need to know basis.

Permanent and full access to live operating environments will be restricted to staff on role-based requirements.

6.3 Controls against Malicious Software

Controls will be implemented to check for malicious or fraudulent code being introduced to critical systems. This will be provided by the external IT Support Company

6.4 Virus Protection

Appropriate software will be installed and managed to prevent the introduction and transmission of computer viruses both within and from outside the School. This will be the responsibility of the external IT support provider.

6.5 Housekeeping

6.5.1 Data Storage

Data on critical systems will be backed up on a daily basis. This service will be provided by the external IT support provider. The provider will be required to present Rambert with a copy of their back up procedures and also clarify arrangements for reinstalling back-ups in the event of server loss.

6.6 Network Management

Controls will be implemented to achieve, maintain and control access to computer networks, including wireless LANs. The SSID for the wireless network must remain hidden and students and staff should be made aware that the network information must not be shared.

Control and access to the Network is granted to the external IT provider, however, that provider must agree to provide written confirmation of their in-house security protocols to prevent unlawful access to the Rambert Network.

6.7 Disposal of Equipment

Removable magnetic and optical media containing key data will be reused or disposed of through controlled and secure means when no longer required.

Procedures will be made to ensure the secure disposal of disk drives and disk packs containing key data when these become defunct or unserviceable.

Redundant computer equipment will be disposed of in accordance with the Waste Electrical and Electronic (WEEE) Regulations and through secure and auditable means.

6.8 Exchanges of Information and Software

6.8.1 Software Usage and Control

Software will be used, managed and controlled in accordance with legislative requirements and the Software Usage & Control Policy in Appendix D

All major software upgrades will be appropriately controlled and tested through a managed process before live implementation. Where appropriate, this will be undertaken by the External IT Support provider

6.8.2 Internet Usage

Activities involving Internet usage, for example e-mail transmission and web site access, will be governed by the Acceptable Use Policy

7. Access control

Access to key data and information will be appropriately controlled.

7.1 User Responsibilities

Subjects who use Rambert's computer systems and/or networks must do so in accordance with the acceptable usage policy

7.2 Requirements for Systems Access

7.2.1 Remote Access

Controls will be implemented to manage and control remote access to key data in accordance with Appendix D

7.2.2 Privilege Management

The allocation and use of system privileges on each computer platform shall be restricted and controlled by the Head of Administration

7.2.3 Passwords

The allocation and management of passwords shall be controlled by the Head of Administration. Users are required to follow good security practices in the selection, use and management of their passwords and to keep them confidential

7.2.4 Unattended User Equipment

Users of IT/IS facilities are responsible for safeguarding key data by ensuring that desktop machines are not left logged-on when unattended, and that portable equipment in their custody is not exposed to opportunistic theft.

Where available, password protected screen-savers and automatic log-out mechanisms are to be used on office based systems to prevent individual accounts being used by persons other than the account holders, but not on cluster computers that are shared by multiple users.

7.3 Monitoring System Access and Use

Access to and use of critical systems will be monitored for both staff and students. Reviewing the information will be the responsibility of the Head of Administration working with the External IT provider.

8 Business continuity management

Controls will be implemented to counteract disruptions to Rambert's information processing facilities and to protect critical systems from the effects of major failures and disruption.

9. Data Storage

Key data will be held on a network resource so that it is backed up through a routine managed process. Where this is not possible, provision must be made for regular and frequent backups to be taken. At Rambert, back-ups are contact out ot eh external IT support provider, who will ensure procedures are in place to restore systems in the event of a system failure.

9.2 Backup Media

A controlled and fully auditable process for the handling, transportation, storage and retrieval of backup media containing key data will be implemented by the External IT support provider

10. Compliance

Controls will be implemented to avoid contravention of legislation, regulatory and contractual obligations and security policy.

10.1 Review of Security Policy

The Policy will be subjected to review annually and in the event of any major changes in circumstances, to ensure those controls remain effective.

10.4 Compliance with Security Policy

Compliance with The Policy is mandatory. Failure to comply with policy requirements, will be viewed as a breach of security. Any such event may be the subject of investigation and possible further action in accordance with Rambert's procedures.

Appendix A - Security responsibilities

A.1 Overall Responsibilities

The Principal of Rambert has responsibility for authorising and reviewing The Policy, and for agreeing all changes. The Head of Administration has been given responsibility for developing and implementing The Policy on behalf of the Principal.

A.2 Rambert School's responsibilities

Rambert school is responsible for:

- Developing The Policy;
- Ensuring that any contracted IT Support Provider adheres to the policy requirements
- Ensuring that the IT Support Provider delivers written copies of their own policies to ensure the security of the Rambert Schools' data and IT infrastructure.
- Ensuring Rambert staff and students adhere to IT policies and procedures
- monitoring and managing compliance against The Policy;
- Ensuring that systems are in place in accordance with the Disaster Recovery/Business Continuity plans, in order to provide prompt and appropriate back-up systems.

A.3 IT Support Providers Responsibilities

The External IT Support Provider is responsible for:

- Providing services and support as per the contractual agreement.
- Providing Rambert School with the following information
    - Confirmation of policies relating to confidentiality
    - Confirmation on processes for informing the school of security breaches
    - Where required provide information on external and internal usage including internet history.
    - Limit, remove or permit access to systems where asked to do so by the Head of Administration.
    - Establishing a process in conjunction with the Head of Administration for the restart of IT systems in the event of a Disaster.

B.4 Individual Responsibilities

Everyone to whom this policy applies has a responsibility to adhere to its requirements.