Ministry of Education

POLICY IN

INFORMATION – PRIVACY AND SECURITY

CONTENTS

INFORMATION - PRIVACY AND SECURITY

1. POLICY OBJECTIVE

The objective of this policy is to ensure proper security, privacy and use of the information within the Ministry of Education (Central Office, divisional Offices, district offices and schools).

2. POLICY

2.1. It is the responsibility of the Ministry of Education staff and private school staff to maintain confidentiality of personal and corporate information.

2.2. Staff are responsible and accountable for maintaining the security of the Ministry's information assets.

2.3. The collection of personal information by the Ministry must be obtained by lawful and fair means and, unless authorised otherwise, must be obtained with the knowledge and consent of the person to whom it relates.

2.4. Persons providing confidential personal have the right to know how it will be used.

2.5. Managers must investigate any complaint any complaint about alleged infringement of information privacy or breach of information security.

3. BACKGROUND

This policy applies to all persons who supply their services to schools in Fiji and all the information gathered by the Ministry and schools other than that which is publicly available.

3.1. Rationale

The Ministry of Education holds an enormous amount of information in hundreds of locations across Fiji. This information is held in Central, Divisional and District offices as well as schools and involves student records, exam results, staff information, business transactions, financial records etc. While much information is available freely to the public, the appropriate security and privacy of this information is also important in order to protect the rights of individuals and uphold the employer/employee confidential relationship.

The Ministry of Education increasingly are conducting business and administration electronically. This brings new challenges for MoE to ensure adequate protection of this information. Measures may include use of passwords and encryption of data. A number of organisations are already requesting the Ministry for access to its corporate information system (School Information Management System – SIMS). While it is appropriate and efficient for some information to be available on-line to some organisations both within government and outside, other information is confidential. For example, confidential information may include teachers' marital status, age and personal addresses and student exam results.

Key principles with respect to confidentiality are articulated in the Public Service Code of Conduct (Part 2, Section 6(10) – Public Service Act 1999)

and the Teachers Code of Conduct. All staff are subject to this code and legislation.

4. RELAVANT LEGISLATION AND OTHER LINKS

General Orders
Education Act

5. PROCEDURES

5.1. Information Use

5.1.1. Personal or corporate information must not be disclosed or made available for purposes other those specified when the data was collected, except with the consent of the persons to whom the data relates or by the authority of the law.

5.1.2. Persons (including the parents of students under 18 years of age) must be told why personal information is being collected and whether it may be accessible to any third party and have their personal information corrected if incorrect or out of date.

Example:

- *School enrolment forms must refer parents to this policy and contain a comment about uses of the information sought.*
- *Computers or filing cabinets containing personal information about employees or students must be secured.*
- *Information given to taxation or FNPF authorities must be limited to the type of data required under the relevant legislation.*
- *Lists showing the names and addresses of employees or students must not be published or supplied except where every person on the list, or in the case of students their parents, have agreed.*

5.2. Information Security

5.2.1. Appropriate security controls, including the use of appropriate receptacles for storage, must be put in place to protect all official or personal information.

5.2.2. Security measures must be reviewed on a regular basis.

5.2.3. Confidential information must be marked and access to it restricted to staff with approved access.

5.2.4. Rights, privileges and authorities made available to employees and contractors of the Ministry must be promptly withdrawn when no longer required.

5.2.5. Records must be kept of authorised security privileges both current and historical.

5.2.6. The risk of loss of or damage to data must be assessed according to accepted risk management principles i.e. classification of data, likelihood of the information being unavailable or subject to unauthorised modification, disclosure or destruction and consequences of data being unavailable or subject to unauthorised modification, disclosure or destruction.

5.3. Electronic Logons and Passwords

5.3.1. Logons and passwords must e kept secure.

5.3.2. All individuals must have their own logon identification or password to access computers and software programs for which they are authorised.

5.3.3. Passwords must change every 30 days.

5.4. Anti-Virus Protection

5.4.1. Worksite managers must ensure there is up to date anti-virus software on all Ministry of Education servers and networked work-stations.

5.5. Disposal

5.5.1. Appropriate security and privacy protection must be undertaken during the disposal of data and records.

6. GUIDELINES

6.1. Disclosure to External Agencies

6.1.1. It is recommended that an official written request for personal information be obtained before it is given to law enforcement agencies or other authorities. However, receipt of a written request does not constitute an obligation to comply with the request. In some cases, legislation is in place which clearly specifies an agency's obligation to release certain information.

6.2. Disaster Recovery and Backups

6.2.1. It is advisable that backup or duplicate copies (paper or electronic) are maintained in secure, off site storage.

6.3. Adherence to Procedures

6.3.1. Work-site managers are advised to circulate a copy of this document to all staff and make sure new staff are shown a copy during their induction to the workplace.

6.3.2. It is recommended that where persons are granted significant security privileges, they be asked to verify in writing their awareness of this policy.

Examples:

- *Persons given keys to rooms with confidential records.*
- *Persons seeking access to computer systems with important, sensitive or confidential information.*

7. EFFECTIVE DATE 1 January 2006

8. REVIEW DATE 1 January 2007

9. KEY SEARCH WORDS

Privacy, information, security, records, password, protection, records management, corporate, logon, access, disposal, data, confidentiality

10. APPROVED BY CEO

SIGNATURE

DATE