



## E-mail Access Policy

### 1 Background

The internal messaging system is intended to provide Ministry of Education & Development (MOED) employees with electronic communications for business purposes.

### 2 Policy Statement

All MOED employees, or persons under contract to the Ministry may be assigned MOED e-mail accounts if the responsible Ministry manager considers it a requirement for the employee's work. Additionally, in the case of a contracted employee, the contract must contain a use of information clause.

All parties with contractual agreements with MOED based primarily off-site to an MOED office who need e-mail for ministry business purposes must use an external Internet Service Provider (ISP) for their e-mail communication service.

All parties with MOED e-mail accounts may be assigned remote access to the MOED messaging system with approval of the responsible Ministry manager based on the requirement for home and travel access.

### 3 Principles

**3.1** Access and use of e-mail must comply with related ITO Information Technology Security Directives and Policies.

**3.2** All executable and macro attachments communicated by e-mail are scanned for viruses by MOED's Mailsweeper system before using.

**3.3** Confidential and sensitive information or information otherwise considered contentious must be secured by encrypting the information. Refer to Appendix A.

**3.5** Ministry information disclosed or received is subject to the *Freedom of Information Act*.



## **4 Responsibilities**

### **4.1 Managers are responsible:**

- to define security requirements in contractual agreements and ensure the security policies are adhered to by any alternate service providers.
- to define contract termination dates for temporary e-mail accounts
- to classify information within the program

### **4.2 Employees are responsible:**

- to adhere to e-mail policies and guidelines .
- to report suspected security problems to the Ministry's IT Manager.
- to apply appropriate security mechanisms for securing information of a confidential or sensitive nature.

### **4.3 Information Technology Department is responsible:**

- to implement expiry dates for temporary e-mail accounts and delete email accounts upon staff exits.
- to provide a secure IT infrastructure environment.
- to monitor e-mail account usage to ensure its use adheres to this policy



## APPENDIX A: Identifying Confidential and/or Sensitive Records

A **record** is information **however recorded**, whether in print, e-mail, voice mail, fax or recorded by any means electronic or otherwise.

The **Freedom of Information Act** – sets out minimum standards which must be consistently applied across the ministry for confidential records which must **not** be disclosed. These include:

- Cabinet and Cabinet related records such as Cabinet Minutes, Cabinet Submissions and Treasury Board Submissions
- Personal information cannot be disclosed without the individual's consent unless required by statute or for law enforcement reasons
- Third party business records whose disclosure could prejudice the business, financial, commercial or other interests of the company
- Briefing materials
- Ministry or government business plans
- Human resources plans
- Business proposals
- Draft legislation and regulations
- Advice and recommendation sections of records
- Legal papers and legal opinions
- Drafts of unpublished policies
- Contract and tender documents
- Labour relations/negotiations records

**This list is illustrative not exhaustive. Each manager is responsible for identifying others within their span of control.**

Records which are, by their nature, contentious must also be properly labelled and secured at all times. **Contentious records** are defined as: "Those whose disclosure would likely result in public debate or discussion". It is important to remember that records are often contentious for only a period of time not necessarily for all time. **Each manager is responsible for remaining current in their identification of the sensitivity and contentiousness of their own records.**