ICT Services Policy of the Ministry of Education 2011
<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>ICT Services Policy</td>
<td>4</td>
</tr>
<tr>
<td>Scope</td>
<td>5</td>
</tr>
<tr>
<td>Intellectual Property rights</td>
<td>6</td>
</tr>
<tr>
<td>Prohibited uses of Computer Resources</td>
<td>6</td>
</tr>
<tr>
<td>Inspection, Monitoring or Disclosure</td>
<td>10</td>
</tr>
<tr>
<td>Responsibility for data Security</td>
<td>13</td>
</tr>
<tr>
<td>Restriction of Access to sensitive data</td>
<td>13</td>
</tr>
<tr>
<td>Violations and Enforcement</td>
<td>13</td>
</tr>
</tbody>
</table>
ICT Services Policy of the Ministry of Education
Ministry of Education (MoE) recognizes its key dependency on the information provided by its computerized system for effective operation and the smooth functionality. It is, therefore, essential that this information and the infrastructure that supports it, is secure from destruction, corruption, unauthorized access and breach of confidentiality, whether accidental or deliberate.

This document is to serve as a set of policies and procedures for the MoE in using ICTs to achieve overall development within organizations and in delivery of its services. It will also ensure consistency in ICT activities and practices.
The Policy is mandatory for providing a unified approach in implementing ICT services and achieving the following;

- Improve efficiency and effectiveness of ICT services of MoE
- Ease of accessibility of MoE information and services for employees, and other citizens
- Promote good governance.
- Develop motivation and ICT competence among MoE employees.
- To encourage the MoE employees to use ICT services ethically.
- Manage ICT resources in sustainable manner.
SCOPE

3.1. This policy defines the boundaries of acceptable use of MoE computing and communication resources, including computers, networks, databases, and electronic mail services.

3.2. Users of MoE computing and communication resources are required to comply with this policy, and other applicable MoE administrative policies and procedures. When necessary, enforcement will be consistent with other applicable Sri Lankan laws.
4.1. In case of a new employee comes to a branch, the head of the branch should inform to Director (ICT) within 2 working days in written format.

4.2. Upon the leaving of an employee, Head of the Branch will raise a Service Request Form (RF) to DE/ICT requesting the e-mail and network resource account to be deleted/transfered/backed up.

4.3. The employee will only be given “user privileges” for their logins. To obtain higher privileges requests with justifications should be made to the Director (ICT) through the proper channel.
5.1. The minimum requirement for a password (for all authentications) is 8 characters.

5.2. Users must maintain the security of their accounts, and are advised to protect and regularly change account passwords.

5.3. Unauthorized attempts to acquire and use passwords of others is prohibited.

5.4. Revealing passwords or permitting the use by others (by intent or negligence) of personal accounts for computer and network access without authorization is prohibited.

5.5. Users are not allowed to share their passwords.
6.1. All computers and network devices of the branches should be connected to the local area network.

6.2. Users must not compromise the integrity of electronic networks, must avoid restricted areas, and must refrain from activities that may damage the network, or transmitted or stored data.

6.3. Interference with or disruption of the computer or network accounts, services, or equipment of others is prohibited.

6.4. Unauthorized scanning of networks for security vulnerabilities is prohibited.
6.5. Attempting to alter any MoE computing or networking components (including, but not limited to, bridges, routers, connection cables and hubs) is prohibited, without approval beyond one’s level of authorization.

6.6. Wiring, including attempts to create network connections, or any extension or retransmission of any computer or network services are prohibited unless approved by the Director (ICT).

6.7. Users should log out of their active sessions on completion of work to prevent unauthorized persons carrying out any activity in the user’s absence.

6.8. Negligent or intentional conduct leading to disruption of electronic network system or information systems is prohibited.
EMAIL

7.1. All employees of the Ministry of Education are entitled to have e-mail accounts.

7.2. It is compulsory to use official e-mail account (organization domain name - moe.gov.lk) for all official e-mail correspondence. Other domain accounts are not valid for official communication.

7.3. All official e-mails should be responded within 2 working days.

7.4. E-mails should be responded to in the language (Sinhala, Tamil or English) in which they are received.
A user must bear responsibility for his or her use of e-mail. MoE can accept no responsibility or liability for any actions of the user or for any consequences resulting from use of e-mail, including but not limited to, misaddressed, lost or undelivered e-mail messages.

Activities that may strain the e-mail or network facilities more than what can be reasonably expected are in violation of this policy. These activities include, but are not limited to: sending chain letters or the widespread dissemination of unsolicited e-mail; and letter bombs to resend the same e-mail repeatedly to one or more recipients.

Confidentiality of e-mail and other network transmissions cannot be assured. Therefore all users should exercise caution when sending personal, financial, confidential, or sensitive information by e-mail or over the network.

E-mails should contain a standard disclaimer. It is as follows.

“This e-mail is confidential. It may also be legally privileged. If you are not the intended recipient or have received it in error, please delete it and all copies from your system and notify the sender immediately by return e-mail. Any unauthorized reading, reproducing, printing, or further dissemination of this e-mail or its' content is strictly prohibited and unlawful. Internet communication cannot be guaranteed to be timely, secure, error or virus-free. The Ministry of Education does not accept liability for any errors or omissions.”
8.1 Branch websites should be hosted within the MoE Web server.

8.2 Each Branch will be provided with “admin privilege” to insert/update/delete the web contents.

8.3 Head of the branch is responsible for the accuracy and quality of the contents in the respective website. If the provided content is found to be not appropriate or harmful to the good name of the MoE, the respective committee shall review such contents.
9.1. Unlawful communications, including threats of violence, obscenity, pornography, and harassing communications, are prohibited.

9.2. Unauthorized anonymous communications are prohibited. All users are required to co-operate with secretary or other authorized personnel when investigating the source of anonymous messages.

9.3. Misrepresenting or forging the identity of the sender or the source of an electronic communication is prohibited.

9.4. Altering the content of a message originating from another person or computer with intent to deceive is prohibited.
Sending of electronic chain mail, denial of service attacks, and inappropriate “broadcasting” of messages to large numbers of individuals or hosts are prohibited.

PROHIBITED USES OF COMPUTER RESOURCES

10.1. Use of MoE computer resources (including printers) for private business or commercial activities, fund raising or advertising on behalf of non-MoE organizations is prohibited.

10.2. Use of MoE computer resources or electronic information without authorization or beyond one’s level of authorization is prohibited.

10.3. Making MoE computing resources available to individuals not affiliated with MoE is prohibited.
10.4. Altering or attempting to alter files or systems without authorization is prohibited.

10.5. Negligent or intentional conduct leading to the damage of MoE electronic information, computing/networking equipment, and resources is prohibited. The computer resources (including printers) may not be used for unauthorized/commercial purposes.

INTELLECTUAL PROPERTY RIGHTS

11.1. Unauthorized use of MoE trademarks or logos and other protected trademarks and logos is prohibited.

11.2. Infringing upon the copyright, trademark, patent, or other intellectual property rights of others in computer programs or electronic information (including plagiarism and unauthorized use or reproduction) is prohibited.
11.3. The unauthorized storing, copying or use of audio files, video files, images, graphics, computer software, data sets, bibliographic records and other protected property is prohibited.

11.4. MoE licenses the use of computer software from a variety of outside companies. MoE does not own this software or its related documentation and unless authorized by the software developer, does not have the right to reproduce it except for backup purposes.

11.5. According to applicable copyright law, persons involved in the illegal reproduction of software can be subject to civil damages and criminal penalties including fines and imprisonments. MoE employees who make, acquire, or use unauthorized copies of computer software shall be
disciplined as appropriate according to the circumstances. Such actions may include termination of the service.

11.6. The Secretary, MoE may permit the inspection, monitoring, or disclosure of e-mail, computer files, and network transmissions when required or permitted by law, including public records law, or by court order.

All computer users agree to cooperate and comply with MoE requests for access to copies of e-mail messages or data when access or disclosure is authorized by this policy or required or allowed by state law or other applicable policies.
RESPONSIBILITY FOR DATA SECURITY

13.1. MoE is not obligated to maintain backups of any files stored in the local machine (local drive). Users must protect and back up critical data.

RESTRICION OF ACCESS TO SENSITIVE DATA

14.1. All branches of MoE should implement policies to ensure that access to sensitive data is restricted to those employees who have a need to access the information. Passwords restricting access to information should be changed on a regular basis.
VIOLATIONS AND ENFORCEMENT

15.1. Any actual or suspected violation of the rules listed above should be brought to the notice of the Director (ICT).

15.2. In case of breach of the ICT services policy, The Secretary, Ministry of Education has the right to terminate the service with immediate effect. Further the Secretary, Ministry of Education has the right to take disciplinary action under the section 2 of establishment code.