# State Service Act 2000

Tasmania

***Ministerial Direction No. 10: 2003***

***Title: INTERNET AND EMAIL USE BY STATE SERVICE OFFICERS AND EMPLOYEES***

| ***Issue Date: 14 OCTOBER 2003*** | ***Operation Date: 14 OCTOBER 2003*** |
|---|---|

## Contents


Contents ..... 1
Purpose ..... 1
Application ..... 1
Legislative Basis and Related Documents ..... 1
Directive ..... 1
Date of period of operation ..... 2
ATTACHMENT 1 ..... 3


## Purpose

The purpose of this Direction is to provide clarity in relation to the appropriate use of Internet and email facilities. Agencies are required to develop and implement appropriate guidelines and user agreements that give effect to the requirements of this Direction.

## Application

This Direction applies to all State Service Agencies, officers and employees.

## Legislative Basis and Related Documents

- *State Service Act 2000*
- *Commissioner's Direction No.5* – Procedures for the investigation and determination of whether an employee has breached of the Code of Conduct

In addition, a variety of legislation exists that prohibits behaviours involving the use of Internet or email facilities. Examples of relevant legislation are provided in Appendix A.

## Directive

Pursuant to Section 14 of the *State Service Act 2000*, I hereby direct that the arrangements outlined in Attachment 1, apply to Internet and email use by State Service officers and employees.

## Date of period of operation

Issued by authority of the Minister administering the *State Service Act 2000* pursuant to Section 14(1).

6/10/2003

Signed

Jim Bacon MHA
***Premier***

Attachment 1

## 1. Introduction

The Crown, as an employer, provides many State Service officers and employees with electronic facilities including Internet access and electronic mail (email) to assist with work related tasks. As owner of these facilities, the Crown has a responsibility to ensure that use is appropriate and complies with all legislative requirements.

To this end, the Crown reserves the right to monitor computer use. This right extends to reading the content of files and emails, including those deleted from an employee's allocated computer.

The purpose of this Direction is to provide clarity in relation to the appropriate use of Internet and email facilities. Agencies are required to develop and implement appropriate guidelines and user agreements that give effect to the requirements of this Direction. Such guidelines may reflect the culture and unique requirements of that Agency and should complement existing Agency information and records management policies and responsibilities.

## 2. Head of Agency Requirements

**2.1** The Head of Agency must ensure that employees and officers provided with access to Internet and email facilities are informed in relation to their appropriate use. In particular, officers and employees are to be made aware of:

(i) the binding nature of this Ministerial Direction, and all other relevant or associated Commissioner's Directions;

(ii) the power under the *State Service Act 2000* to sanction employees and officers who breach the Code of Conduct;

(iii) the retention of property rights by the Crown;

(iv) the capacity of the Crown to monitor computer use including internet and email; and

(v) the potential implications for the Crown arising from the misuse of email and Internet facilities by the individual e.g. the transmission of information to unintended recipients.

Officers and employees are to be made aware that any use of Internet and email facilities which contravenes the *State Service Act 2000*, or any other legislation identified in Attachment A of this Direction, will constitute misuse. Misuse includes, but is not limited to the following:

(i) downloading excessive information for personal use or otherwise using facilities to the detriment of the Agency's efficient operation;

(ii) initiating or forwarding defamatory, offensive or harassing emails;

(iii) displaying or transmitting pornographic, obscene, or other objectionable material;

(iv) undertaking private commercial activities using departmental facilities;

(v) gaining unauthorised access to other systems;

(vi) downloading and/or installing unlicensed software without appropriate Agency approval;

(vii) unwarranted or unauthorised access, duplication, or distribution of client, staff or Agency information or records;

(viii) using facilities for the initiation and/or distribution of unauthorised and unsolicited information of a political or commercial nature; and

(ix) forging or misrepresentation of identity using electronic facilities.

It should be noted that while some uses of Internet and email facilities might not of themselves be illegal (eg downloading and viewing some types of pornographic material), they are inconsistent with community expectations of State Service officers and employees and are not considered an appropriate use of government resources.

**2.2** The Head of Agency must develop Agency specific Internet and electronic mail guidelines consistent with the framework provided by this Ministerial Direction. In formalising such guidelines, the Head of Agency should consult with officers and employees and with the Solicitor-General. The guidelines should *specifically* determine:

i) the type of personal use permitted to employees;

ii) the extent to which appropriate personal use will be allowed (i.e. times and duration);

iii) the form and use of appropriate disclaimers on outgoing transmissions;

iv) how use will be monitored i.e. regularly, randomly, or by exception (e.g. in response to complaints or investigations) and;

v) who in the Agency will be responsible for and permitted to undertake monitoring (i.e. those positions that can authorise monitoring and those positions that can undertake the monitoring function).

**2.3** The Head of Agency must develop an Agency specific Internet and electronic mail usage agreement for all employees and officers provided with access to Internet and email facilities. This must verify that the officer or employee has been made aware of the content of this Direction, Agency guidelines, and understands their rights and responsibilities.

**2.4** The State Service Commissioner is to be provided with a copy of the approved Agency guidelines.

**2.5** A Head of Agency must review the Agency's Internet and electronic mail guidelines and associated agreements at least every four years. The State Service Commissioner must be provided with a report of this review process within six months of the review due date.

## 3. Sanctions for Misuse

Sanctions for misuse of Internet and email facilities will vary depending on the nature and seriousness of the misuse.

(a) Where misuse constitutes a contravention of law in Tasmania, evidence should be provided to the relevant external authority. Internal action under the *State Service Act 2000* may also be taken in accordance with (b).

(b) Where misuse constitutes a breach of the Code of Conduct (Section 9 of the *State Service Act 2000*), any action taken must be in accordance with *Commissioner's Direction No. 5* – Procedures for the investigation and determination of whether an employee has breached the Code of Conduct.

(c) Where the nature or the seriousness of the misuse does not constitute a breach of the Code of Conduct, action may be taken in accordance with Section 2 of *Commissioner's Direction No. 5* – Procedures for the investigation and determination of whether an employee has breached the Code of Conduct and *Commissioner's Direction No. 4* – Performance Management.

## 4. Head of Agency Discretion

The Head of Agency retains the discretion to determine if misuse has occurred inadvertently.

## Appendix A - Legislation Relevant to Internet and Email Use

| **Action** | **Relevant legislation** |
|---|---|
| Defraud others | Use a computer with intent to defraud (see S.257B *Criminal Code 1924* and S.43A of the *Police Offences Act 1935*) |
| Create or intentionally distribute viruses | Damage computer data (see S.257C *Criminal Code 1924* and S.43B of the *Police Offences Act 1935*) |
| Breach copyright | Download, transmit, or publish material that is in breach of copyright (see *Copyright Act 1968* (Cth)) |
| Distribute defamatory material | Use of the Internet or email to transmit or publish material that is defamatory (see *Defamation Act 1957*). |
| Offend or ridicule others | Use of the Internet or email to engage in conduct that offends, humiliates, intimidates, insults or ridicules on the basis of gender, marital status, pregnancy, breast feeding, parental status or family responsibilities (see S.17 of the *Anti-Discrimination Act 1998*). |
| Incite hatred | Use of the Internet or email to incite hatred, serious contempt or sever ridicule on the grounds of race, disability, sexual orientation or lawful sexual activity or religious belief, affiliation or activity (see S.19 of the *Anti-Discrimination Act 1998*). |
| Promote discrimination | Publish or display or cause to be published or displayed any sign, notice or advertising matters that promotes, expresses or depicts discrimination or prohibited conduct under the Anti-Discrimination Act 1998 (see S.20 of the *Anti-Discrimination Act 1998*) |
| Assist others to break the law | Use of the Internet or email to publish or transmit material that may assist others in the commission of criminal offences (see *Criminal Code 1924*) |
| Distribute Pornography | What is illegal off line is illegal online. Therefore, the viewing of some forms of sexually explicit adult material may not be of itself illegal, however, unsolicited distribution or display of this material may be in breach of the Anti-Discrimination Act (S.17 of the *Anti-Discrimination Act 1998*). |
| Run a business | Engage in running or supporting private commercial activities using departmental facilities and resources (S.9 of the *State Service Act 2000*). |
| Public statements | Use of the Internet or email to make public comment on any matter affecting the Agency in which an officer or employee is employed (*State Service Regulations* S.11) |
| Stalking | Engage in conduct with the intention to cause harm, fear or apprehension of fear (*Criminal Code Act 1924*) |
| Gaming | Engage in forms of gaming that are prohibited under the *Interactive Gaming Act 2001* eg. interactive gaming including micro-wagering and highly repetitive or frequently drawn lotteries. |

*The above list is not exhaustive, but indicates the type and range of legislation relevant to Internet and email use.*