

1. Title: Use of Internet and Electronic Mail Policy and Principles Statement

2. Effective Date: 7 September 2007

3. Date of Issue: 7 September 2007

4. Policy:

The internet and electronic mail (email) are important sources of information and means of communication that can assist government to provide more effective services to the community. The use and/or access to these must be able to survive public scrutiny and/or disclosure.

The provision of internet and email facilities and devices are for officially approved purposes. Limited personal use of internet and email facilities and devices should be available on a basis approved by the agency's chief executive officer.

Limited personal use is generally expected to take place during the employee's non-work time, incurs minimal additional expense to the government, is infrequent and brief, does not interfere with the operation of the government and does not violate any State/agency policy or related State/Federal legislation and regulation.

Employees are accountable to their employing agency for the use of these technologies. Employees found to be intentionally accessing, downloading, storing or distributing pornography using government-owned information and communication technology (ICT) facilities and devices will be dismissed.

Employees may also be disciplined or dismissed for the misuse of the internet or electronic mail in respect of material which is offensive or unlawful, although not pornographic. A pattern of behaviour (for example, repeated use) is a factor for consideration in determining disciplinary measures (including dismissal).

Employees are defined as those engaged on a tenured, temporary, or seconded basis as defined by the *Public Service Act 2008* and/or relevant agency legislation. Where contractors are engaged to provide services for, or on behalf of, the agency, contract conditions must clearly reflect the government's policy on this issue. Agencies must ensure that other persons, such as students, volunteers, work experience, or other external bodies authorised by the agency to use government-owned ICT facilities and devices, are aware of and acknowledge the government policy on the restrictions and consequences of misuse of these facilities and devices.

5. Principles:

5.1 Agency Responsibilities

When managing and monitoring the use of internet and email facilities and devices, agencies must:

- Ensure appropriate and ongoing training of employees in their responsibilities concerning internet and email use policies and practices;

- Ensure policies, practices and systems are in place that are consistent with ethical and legal obligations;
- Reduce security risks including the disruption to agency operations and unauthorised use (intentional or unintentional) by employees;
- Ensure disciplinary procedures and penalties imposed on employees for breaches of internet and email use are clear, unambiguous, proportionate to the offence and are applied in a manner which is timely, fair and decisive;
- Ensure that the penalty for intentionally accessing, downloading, storing or distributing pornography is communicated to all employees in clear and unambiguous language;
- Clearly address procedures and practices for reporting potential breaches of the law to the relevant law enforcement authority and report suspected official misconduct to the Crime and Misconduct Commission;
- Address issues relating to the record keeping, archiving, privacy, freedom of information and audit requirements of internet and email monitoring; and
- Ensure employees are aware that, when receiving unsolicited inappropriate material from the internet or through an email, they delete such material from agency systems immediately. Action to delete this material would not constitute unauthorised use.

5.2 Agency Policy

Agencies must develop, implement and communicate clear and unambiguous policies and guidelines addressing the use and monitoring of internet and email within the agency. At a minimum, agencies must ensure that these policies and guidelines:

- Are consistent with Commonwealth legislation, the Queensland Government Information Standards, the *Public Sector Ethics Act 1994* and the agency's approved code of conduct;
- Are reviewed on an ongoing basis, are readily accessible and regularly communicated to all employees;
- Define which employees within the agency are authorised to use internet and email, and the conditions and constraints relating to their use in terms of agency security, privacy, copyright, confidentiality and delegation policies;
- Define what internet and email will be monitored and the conditions under which this monitoring will take place;
- Define what is considered authorised and unauthorised use and provide clear definitions, comprehensive examples and permitted levels of such use;
- Define the range of disciplinary procedures and penalties which may be applied as a consequence of unauthorised use of internet and email including that the penalty in the case of an employee being found to have intentionally accessed, downloaded, stored or distributed pornography using government-owned ICT facilities and devices is, subject to industrial and procedural fairness, termination of employment; and
- Define who has access to monitoring reports and the delegation chain of authority for dealing with reports generated from this activity.

5.3 Employee Responsibilities

Internet and email usage must be able to survive public scrutiny and/or disclosure, and, in their use of internet and email facilities and devices, employees must not use these facilities or devices to:

- Defame, harass, abuse or otherwise offend other internet and email users, individuals, government agencies or other organisations;
- Refer to people in a manner that could reasonably be taken by them as being offensive;
- Knowingly access inappropriate internet sites and activities;
- Intentionally access, download, store or distribute offensive material (e.g. pornography, inappropriate pictures, literature, games or videos), unlawful or criminal material or material containing defamatory comments;
- Create or distribute any form of malicious or deleterious material via the internet or email;
- Attempt to obscure the origin of any message or download material under an assumed internet address or otherwise disguise the user's identity;

- Knowingly obtain unauthorised access to information or damage, delete, insert or otherwise alter such information with malicious intent;
- Infringe copyright or unlawfully circumvent technological protection measures designed to deter copyright infringement;
- Maintain or support a personal private business; and
- Disrupt communication and information or degrade network services by sending unsolicited commercial electronic messages (spamming), other junk email including chain email or other inappropriate use.