

# South Bank Corporation Policy

## Corporate Services

**SUBJECT:** Intranet, Internet and Email Usage Policy  
**DATE CREATED:** March 2005  
**REVIEW DATE:** September 2007

### Introduction:

The purpose of this policy is to advise the conditions concerning the use of the Intranet, Internet and email services provided by South Bank Corporation. The public sector ethics principles addressed are respect for persons, integrity, and economy and efficiency. The Corporation will not condone inappropriate use of Corporate resources. Failure to comply with these policies may result in disciplinary action including dismissal.

### Scope:

This document details the acceptable use policies applicable to all users who have access to South bank Corporation electronic information services.

The standards of acceptable use prescribed in this policy apply to every user, regardless of the technical method, location and or access means by which that user has connected to the network.

### Terminology:

- Users – employees, contractor or external parties that have been granted a valid username and password that allows access to the Corporation network and associated systems.
- Electronic communications systems – these include the Internet, voice mail, electronic mail, and fax.
- The Internet or Internet services – the provision of access to the Intranet and Internet from the Corporation's network.

### Procedures:

The granting of access is subject to the users understanding of, and agreement to comply with, current policies and relevant procedures concerning the use of the Internet services. All users of South Bank Corporation network have access to the Internet and Email and the ability to copy material and save it to disk.

Users are to use this access for Corporation business or for the professional development, but are not authorised to use it for other business or for personal financial gain or excessive personal use.

The granting of access to the Internet and Email is to be authorised by the appropriate manager who will take into account the person's need or the benefit of such access. Access requirements will be reassessed where the user's job description or role changes.

#### 1. Company Property

Policy: As a productivity enhancement tool, the Corporation encourages the business use of electronic communications. Electronic communications systems and all messages generated on or handled by electronic

communications systems, including back-up copies, are considered to be the property of the Corporation.

## 2. Authorised Usage

Policy: The Corporation's Internet services should generally be used only for business activities. Incidental personal use is permissible as long as it:

- (a) Does not consume more than a minimal amount of resources,
- (b) Does not interfere with employee productivity, and
- (c) Does not pre-empt any business activity.

Users are forbidden from using the Corporation's electronic communication systems for charitable endeavours, private business activities, or amusement/entertainment purposes. Employees are reminded that the use of corporate resources, including electronic communications, should never create neither the appearance nor the reality of inappropriate use.

### **Corporation Responsibilities:**

#### 1. Communication

The Corporation will inform all staff of their responsibilities in respect of the Intranet, Internet and email Usage Policy.

#### 2. Inbound Attachments to Internet Electronic Mail Prohibited

Policy: Attachments to inbound Internet electronic mail messages sent to Corporation users and deemed unsuitable or posing a security threat will be automatically deleted. If an executable program or some other non-text message must be received, other methods must instead be employed under the supervision of the IT Co-ordinator.

### **Users Responsibilities:**

#### 1. User ID's and Passwords

Policy: Users should keep their userids and passwords secure. They should not reveal to others, nor allow others to use, their userids or passwords. It is considered good practice to change passwords on a regular basis; hence the domain security policy will prompt for a password change every 55 days.

#### 2. Using an Electronic Mail Account Assigned to Another Individual

Policy: Users must not use an electronic mail account assigned to another individual to either send or receive messages. If there is need to read another's mail (while they are away on annual leave for instance), message forwarding and other facilities must instead be used.

#### 3. Profane, Obscene or Derogatory Remarks in Electronic Mail Messages

Policy: Users must not use profanity, obscenities, or derogatory remarks in electronic mail messages discussing employees, customers, or competitors. Users should not use the intranet, Internet or email in a way that could defame, harass, abuse or offend other intranet, Internet and email users, individuals or organisations. Apart from constituting a breach of policy, such remarks -- even when made in jest -- may create legal problems such as trade libel and



defamation of character. Special caution is warranted because back-up and archival copies of electronic mail may actually be more permanent and more readily accessed than traditional paper communications.

#### 4. User Retention of Electronic Mail Messages for Future Reference

Policy: If an electronic mail message contains information relevant to the completion of a business transaction, contains potentially important reference information, or has value as evidence of a Corporation management decision, it must be retained for future reference. Legislation and regulations that directly relate to public recordkeeping in Queensland include:

- Electronic Transaction Act 2001;
- Evidence Act 1977;
- Financial Administration and Audit Act 1977;
- Financial Management Standard 1977;
- Freedom of Information Act 1992;
- Judicial Review Act 1991;
- Public Records Act 2002; and
- Public Service Act 1996.

#### 5. Users Must Not Employ Electronic Mail Systems as a Database

Policy: Users must regularly move important information from electronic mail message files to word processing documents, databases, and other files. Electronic mail systems are not intended for the archival storage of important information. Stored electronic mail messages may be periodically expunged by systems administrators, mistakenly erased by users, and otherwise lost when system problems occur.

#### 6. Privacy Expectations and Electronic Mail

Policy: Users must treat electronic mail messages and files as private information. Electronic mail must be handled as a private and direct communication between a sender and a recipient.

#### 7. Treat Electronic Mail as Public Communications

Policy: Consider electronic mail to be the electronic equivalent of a postcard. Unless the material is encrypted, users must refrain from sending credit card numbers, passwords, and other sensitive data via electronic mail. Electronic messages and electronic files are subject to record keeping, archiving, freedom of information and legal process.

#### 8. Message Content Restrictions for The Corporation Information Systems

Policy: Users are prohibited from sending or forwarding any messages via the Corporation information systems that a reasonable person would consider to be defamatory, harassing, or explicitly sexual. Users are also prohibited from sending or forwarding messages or images via the Corporation systems that would constitute discrimination. Users should not create, knowingly access, download, distribute, store or display any form of offensive, defamatory, discriminatory, malicious or pornographic material.

Material which contains viruses, worms, "Trojan horses", or any other contaminating or destructive features must not be posted or transmitted. No form of computer hacking is permitted.

#### 9. Notification of Content Monitoring for Electronic Mail Transmissions



Policy: The Corporation routinely employs automatic electronic mail content scanning tools to identify selected keywords, file types, and other information. Users should restrict their communications to business matters in recognition of this electronic monitoring. The Corporation reserves the right to monitor and audit any or all intranet, Internet or email activity undertaken by users using Corporation resources. Users may be called on to explain their use of the intranet, Internet or email.

South Bank Corporation may monitor usage of the Internet by employees. No individual should have any expectation of privacy in terms of their usage of the Internet on company property.

#### 10. Electronic Mail Messages Are Company Records

Policy: Intranet, Internet and email access is provided for officially approved purposes only i.e. Corporation business and limited personal use. All messages sent by electronic mail are the Corporation records. The Corporation reserves the right to access and disclose all messages sent over its electronic mail system, for any purpose. Management may review the electronic mail communications of users they supervise to determine whether they have breached security, violated Corporation policy, or taken other unauthorised actions. The Corporation may also disclose electronic mail messages to law enforcement officials without prior notice to the users who may have sent or received such messages.

#### 11. Personal Use of Electronic Mail Systems

Policy: Electronic mail systems are intended to be used primarily for business purposes. Any personal use must not interfere with normal business activities, must not involve solicitation, must not be associated with any for-profit outside business activity, and must not potentially embarrass the Corporation.

Intranet, Internet and email usage should be able to withstand public scrutiny and/or disclosure. Unauthorised access, transmittal or storage of material that might bring the Corporation into disrepute is prohibited.

#### 12. Unauthorised access to Internet Services infrastructure

Policy: Users should not disrupt or interfere with the use of intranet, Internet or email services. Users should not attempt any unauthorised access of intranet, Internet or email services. Unauthorised access includes, for example, the distribution of messages anonymously, use of other employees' userids or using a false identity.

The Corporation has security arrangements in place to protect the network from unauthorised access. Employees are required to support these security arrangements.

Access to the internet should be via officially approved mechanisms only. The connection of stand-alone modems to individual personal computers must be authorised on a case-by-case basis by management.

#### 13. Corporation information usage

Policy: Users must comply with all policies, legislation and regulations applicable to the use of the intranet, Internet and email. The Corporation information should not be transmitted or made available via the intranet, Internet or email except



under Corporation approved protocols. Violations of Corporation policy may result in restriction of access to technologies, disciplinary action (including dismissal) and/or action by the relevant regulatory authorities.

Users should not knowingly obtain unauthorised access to information and should not damage, delete, insert or otherwise alter such information carelessly or with malicious intent.

#### 14. All Information Posted on Intranet Pages Must Have Designated Owner

Policy: All information posted to the Corporation intranet automatically has a designated owner assigned.

#### 15. All Content Posted to Intranet is Owned by Corporation

Policy: All content posted to the Corporation intranet is the property of the Corporation.

#### 16. Permission Required for Intranet Posting

Policy: Before any information is posted to the Corporation intranet, the appropriate approvals must be obtained. First, the department manager in charge of the relevant area to which the intranet page content relates must approve it. Second, the owner of the involved information (or creator of the information if the owner has not yet been designated) must approve.

#### 17. Prohibition Against Use of Scanned Hand-Rendered Signatures

Policy: Users must not employ scanned versions of another party's hand-rendered signatures to give the impression that an electronic mail message or other electronic communications were signed by the sender.

#### **Message:**

The Corporation will add the following message to each outgoing email:

'This email and any files transmitted with it are confidential and intended solely for the use of the individual or entity to which they are addressed. If you are not the intended recipient, any use, interference with, disclosure or copying of this material is unauthorised and prohibited. Please note that any views or opinions presented in this email are solely those of the author and do not necessarily represent those of the Corporation. Finally, the recipient should check this email and any attachments for the presence of viruses. The Corporation accepts no liability for any damage caused by any virus transmitted by this email.'

E-mail correspondence sent from the Corporation or addressed to it will be treated as a public record and will be retained as required by *The Public Records Act 2002* and other relevant regulations.

Except where you indicate otherwise, your name and address will not be added to any mailing list. We will not disclose anything about you to third parties without your consent unless required by law. E-mail messages may be monitored by our Internet Service Provider for system troubleshooting and maintenance purposes.'

#### **Declaration:**



I have read, understood and acknowledge receipt of the Intranet, Internet and Email usage Policy. I will comply with the guidelines set out in this policy and understand that failure to do so might result in disciplinary or legal action.

Signature: \_\_\_\_\_ Date: \_\_\_\_\_

Printed Name: \_\_\_\_\_