

1. Policy Statement

- 1.1 The organisations participating in the ease to e working initiative have utilised information technology and 'leading edge' technology in order to participate in the project. Easy access to and use of such technology is essential to each organisations ability to provide superior customer service. All participating organisations expect their employees to exercise common sense and good judgement whilst using all of their technology resources for business purposes. They expect that if all employees act responsibly and ethically the participating organisations can continue to provide the current level of access.
- 1.2 Users who engage in practices or who have material which is in contravention of this policy should take immediate action to remove/delete that material.

2. Introduction

- 2.1 The participating organisations provide electronic communications equipment and services for the performance of tasks related to employees work. Limited personal usage, providing it is a specified within other guidelines, remains acceptable.
- 2.2 Examples of such equipment and services are telephone, fax, voice mail, computers, e-mail, Internet, and other electronic communication links whether they are on site, mobile, or remote. All business use of e-mail must be performed on the participating organisation's-provided e-mail systems.
- 2.3 Business use of non-organisation provided e-mail systems is strictly prohibited. This includes the use of Web based e-mail such as Hotmail, Yahoo-mail, etc.
 - 2.3.1 There should be no expectation of personal privacy when using the participating organisation's equipment and services. All information, data or files created, received, downloaded, stored, transmitted, deleted or used while in the employ of the participating organisation are the participating organisation's property.

3. Monitoring of Information Flows

- 3.1 It is good practice to put in place arrangements which provide the facility to audit information in various electronic formats in order to safeguard the interests of employees and fulfil statutory obligations. Electronic format encompasses both information transmitted in real time as well as historical information.
- 3.2 The participating organisations may monitor, copy, access, or disclose any information or files that employees create, receive, download, store, transmit, delete or work with while using the participating organisation's equipment and services including, but not limited to:

- *Verifying performance or quality; assuring compliance with the participating organisation's policies and procedures;*
- *Routine scanning of email to isolate messages containing unwanted and unacceptable text and/or images*
- *Detecting improper use or conduct that may be illegal or adversely affect the participating organisations, and their contractual relationship with their customers or their employees; and,*
- *Preventing inappropriate or excessive personal use of the participating organisation's equipment.*

This monitoring may be periodic, random or continuous. The participating organisation may investigate any transmission or storage of information and any use of equipment or services inconsistent with the participating organisation's ownership interests.

3.2 While the participating organisations do not routinely monitor e-mail, they may do so for the following reasons:

- *To detect viruses or other malicious content*
- *To locate information urgently required for the participating organisation's business*
- *To respond to legal or regulatory requirements*
- *To fulfil their obligations to customers, third parties and relevant regulatory authorities*
- *In the course of an investigation triggered by indications of misconduct*

3.3 Such monitoring of e-mail will be authorised by a designated senior manager in the participating organisation and notified to the relevant responsible authority.

4. Improper use of the participating organisation's equipment

This includes the following:

- 4.1 Using equipment or services for-viewing, transmission, storing, downloading or communication of images or text consisting of –
 - *ethnic slurs, racial epithets, hate speech, sexually explicit or provocative material, obscenities, or anything else that may be construed as illegally harassing or offensive to others based on-*
 - *an individual's race, national origin, religion, sex, sexual orientation, colour, marital status, age, disability, or any other legally protected category;*
- 4.2 Accessing sites and 'chat rooms' that feature gambling, pornography, off-colour jokes, hate speech and similar sites; or, any solicitation or distribution unrelated or contrary to the participating organisation's interests.
- 4.3 Viewing, storing or propagating of any form of material that could be construed as pornographic.
- 4.4 Transmission of any statements or materials which are defamatory, abusive, obscene, or which may cause offence or annoyance to any other person.
- 4.5 Offensive screensavers are strictly prohibited.
- 4.6.1 Such conduct is inconsistent with the professional environment that the participating organisations strive to maintain. If an employee has engaged in improper use, he or she should assume that he or she will be subjected to the participating organisation's disciplinary procedure

up to and including dismissal and/or legal proceedings.

- 4.6.2 The participating organisations' computer and network resources are business tools. As such, they must not be used to send or forward threatening or harassing messages or chain letters, or to express personal opinions on behalf of the participating organisations in on-line forums. Employees' personal opinions or feelings must not be submitted to these media. This is an area where misguided or ill-informed activity could seriously damage the reputation of the participating organisations.
- 4.7 If an employee receives a communication which contains inappropriate messages they must inform the sender that such material is not permitted under the participating organisation's policy on electronic communication.
- 4.8 It is strictly prohibited to forward inappropriate material of any nature.
- 4.9 It is prohibited to download commercial software that has not been legally licensed by the participating organisations.

5. Commercial sensitivity.

- 5.1 The participating organisations recognise that email is becoming an increasingly important tool for communicating with customers, vendors, and other parties outside of the participating organisations and this policy is not intended to prohibit email communications with parties outside the participating organisations. It is intended, however, to protect organisation confidential, proprietary information, as well as the privacy interests of employees of the participating organisations.
- 5.2 Any communication sent by e-mail may be subject to a discovery order by the courts and may be disclosed to any relevant authority, unless the e-mail comes within the category of communications protected by legal privilege e.g. in the context of advice sought from the organisations solicitors in anticipation of litigation or in the course of legal proceedings
- 5.3 The participating organisations rely on email as an efficient means of communicating information to its employees. Although email may appear to be a more informal method of communicating, it has the same legal effect as other written communications. Employees should thus exercise discretion when sending an email note and choose their words with the same care that they would use when sending a formal letter or written memorandum.
- 5.4 Additionally, email often contains commercially sensitive, proprietary and confidential information about the participating organisations. On any given day, for example, the participating organisation's email may announce organisational changes, business goals, product availability, product directions, recent customer wins, current customer prospects, internal policies and strategic competitive analyses, none of which is public information.
- 5.5 Email notes among individual employees are likely to discuss similar issues even less-guardedly and with more candour. In addition, email notes among employees may contain personal information that the initial sender never intended for widespread distribution beyond the initial recipients.
- 5.6 An employee's contract with the participating organisation obligates them to keep confidential any proprietary information. This includes email. Accordingly, no internal email, except that which clearly on its face is intended for public distribution (e.g. Press Releases), should be sent to

any party outside of the participating organisation. The presumption is that all email communications are confidential and for internal use only UNLESS it is clear from their content that they are intended for distribution to persons outside the participating organisation.

- 5.7 In addition, an employee may not establish an 'automatic' forward of electronic mail to an address outside the organisation's domain. This includes, for example, the auto-forwarding of an employee's organisational email to a personal email account with an outside provider or to an email account that the employee may maintain at a client site. This policy is intended to protect confidential information of the participating organisations by preventing the unauthorised transmission or disclosure of internal communications to unauthorised parties outside. The participating organisations may monitor their email systems for auto-forwarding.

6. Internet Usage.

- 6.1.1 The Internet and World Wide Web are an important resource to those organisations participating in the ease to e working project, providing improved communications, useful information and the opportunity to reach customers as never before. All communications must comply with applicable laws and regulations, including those governing the export and import of technology, software, and the protection of copyrights and intellectual property generated.
- 6.1.2 For further information on Internet Usage please consult the IT support person in the relevant participating organisation.

7. Scope

- 7.1 This policy applies to all those who have access to the participating organisations' communications resources (including, employees, contractors, consultants, visitors, and others not specifically mentioned).

8. Responsibility

- 8.1 It is the responsibility of all employees to make themselves aware of this policy and to follow the participating organisation's procedure as outlined.
- 8.2 Employees engaging in unauthorised activities and who breach the requirements of this policy may be subject to disciplinary procedure, up to and including termination of employment, and/or legal proceedings.