Email & Internet Use Policy

1.0 Purpose

The purpose of this policy is to define acceptable email and internet use within working time.

2.0 Email and internet use for work purposes

Many employees will be required to use email and the internet regularly for work purposes. This is clearly acceptable when it is fulfilling work duties. However, it is important that employees are mindful of the need to use email and the internet appropriately. In particular:

- No obscene or offensive language should ever be used in emails;
- Emails of a discriminatory, derogatory or defamatory nature must never be sent;
- Email must never be used as a form of communication which could cause harassment or be abusive to someone;
- Emails should not be copied to people inappropriately;
- If an employee receives an offensive email this should be reported to his/her line manager. It should not be passed on to other employees;
- Employees are permitted to access internet sites at work except for content expressly stated as prohibited in this policy
- Email content and language should remain consistent with the organisation's best practice;
- Email messages should remain concise and appropriate.

    If you do use email inappropriately including some of the examples above, you may be liable to disciplinary action up to and including summary dismissal.

    During an employee's absence (for holiday, sickness or any other reason) the organisation reserves the right to access the employee's email account. This is necessary to ensure that any business issues are addressed in a timely manner.

3.0 Email use for personal purposes

During official breaks (e.g. lunchtime) employees may access their personal email accounts. However, in responding to emails the code of conduct relating to work emails (as explained above) applies.

4.0 Internet use for personal purposes

During official breaks (e.g. lunchtime) employees may access the internet for personal use. However, only appropriate sites may be accessed (see below).

5.0 Internet sites that cannot be accessed

Under NO circumstances can any pornographic internet site be accessed during working hours or at any time using a computer belonging to the organisation. Any other internet sites that contain offensive, obscene or otherwise unacceptable material must not be accessed using a computer belonging to the organisation, or during working hours.

6.0 Downloading of material

Viruses and similar problems can bring an entire computer network to a standstill. It is important, therefore, that all employees are aware of the need to act responsibly and minimise the risk of this occurring. To help

protect the company network, employees must not download any documents on to a computer belonging to the organisation without being confident that it comes from a legitimate and trusted source.

No software can be downloaded onto a computer belonging to the organisation without the express agreement of a Company Director.

7.0 On-line blogs

Whether during business hours or personal time, employees must not contribute to any blog which criticises the organisation, or otherwise brings the organisation into disrepute. If the employee is dissatisfied with some aspect of their employment this should be addressed using the organisation's grievance procedure details of which are contained within the Employee Handbook.

Using a blog to criticise or damage the reputation of the organisation may result in disciplinary action

8.0 Storage of emails

The Data Protection Act 1998 requires that information that is recorded is not excessive, is not kept for longer than necessary and is relevant. Employees, therefore, are required to archive their emails appropriately and to delete information that is no longer required.

9.0 Copyright

Copyright rules do apply to articles on the internet. Hence, care should be taken when using internet information. If there is any doubt whether material can be used then advice should be sought from a Director of the Company.

10.0 Organisation's website

No employee may add any information to the organisation's website without express consent of the Director responsible for the website.

11.0 Monitoring

The organisation reserves the right to monitor the email and internet use on any computer which belongs to the organisation.

12.0 Action to be taken in the case of inappropriate use

If an employee is found to have used email or the internet in an inappropriate manner disciplinary action may be taken. This could include summary dismissal, depending on the nature and severity of the offence.

13.0 Bullying and Harassment

If an employee feels that they are being harassed or have been harassed or bullied or are offended by material received from a colleague, the employee should immediately inform their line manager of the situation.

14.0 Authorisation

The authority for this policy is vested in the Managing Director.

Alan Jones

Document Control
A hard copy of this policy is kept at Head Office.