Falcon FoodService Equipment
Internet Acceptable Usage Policy

CHAPTER 1 PREFACE

AFG's policy is always to comply with the relevant law in the jurisdictions in which it operates. This is an overarching principle, which should guide the actions of the company & employees.

This document has been issued by Falcon FoodService Equipment to ensure that the company's internal controls stay abreast of the changes brought about through the increased use by employees of company-provided computers and Internet connections. The fact that it has been issued should not be taken to imply that such computers and connections are currently being misused, but rather that the company recognises the need to keep pace with developments in the environment in which it operates.

CHAPTER 2 GENERAL

AGA FoodService Group recognises equally the benefits that may accrue from use of the Internet as a business tool throughout the Group and the risks posed to its business by the Internet and other high speed means of electronic communication. Whilst not exhaustive, the following are of legitimate concern to the Group:

- The ease, with which inappropriate material may be accessed.
- The ease with which information may be disseminated.
- The ease with which damaging and/or unlicensed software can be obtained, both intentionally and non-intentionally.
- The disruption that may be caused by use of this business tool for personal purposes.

In this policy "inappropriate" includes all material that is offensive and/or obscene and any derogatory or inflammatory references and comments, especially those pertaining to Race, Gender, Creed, Appearance and Disability.

- Additionally, "inappropriate" expressly includes communicating with minor children, or other persons, regarding immoral or illegal activities, or with a view to engaging in such activities in the future.
- In many jurisdictions, the originators and disseminators of such material, including the Group if its equipment is used, are liable to prosecution.

The use of a company-provided Internet connection or computer to access, display, print or transfer pornographic or other inappropriate material whether by e-mail, World Wide Web, file transfer or other means is expressly prohibited.

When accessing the Internet from Falcon FoodService systems, employees represent Falcon FoodService and the Group and use must therefore be appropriate and behaviour professional at all times.

Falcon FoodService does not prohibit the reasonable and limited use of a company provided Internet connection by employees in their personal capacity. However, such connections are provided for the benefit of the Group's business and local management has the authority to

prohibit or restrict such use at its own discretion.

Employees are reminded that communications emanating from company-provided mailboxes and Internet connections expose the company to legal risks and commitments as if they had been written on letter headed paper.

Only personnel who normally have authority to place such orders may order goods or services over the Internet and each business's normal procedures for placing purchase orders and authorising payments, must also be complied with.

Employees should obtain permission from their manager before participating in Internet discussion groups or subscribing to other Internet services.

- Employees participating in discussion groups do not have authority to represent their views as being those of Falcon FoodService, or any other member of the AFG group, or the Group as a whole and any such postings must clearly state that they are the personal opinions of the author.

Due regard must be given to the need to preserve commercial confidentiality when using computers or the Internet.

- Employees should be aware that the Internet is a mass publication medium and that there is no guarantee that communications issued will be treated as private by their recipients. Particularly, electronic mail can readily be copied and forwarded to other people and organisations.

- Information transferred on the Internet is not secure by default. Never transfer anything that you want to keep private, such as a credit-card number, or that which is confidential, without taking precautions, e.g. the use of encryption or an SSL Web page – these are denoted by a picture of a closed padlock at the bottom of the screen.

Programs and documents downloaded from external sources may contain harmful viruses. Each person receiving Word Processing documents, spreadsheets and binary or executable files, is individually accountable for observing appropriate measures to ensure the safety of such files prior to their use on company computing facilities.

Users should make periodic checks to ensure that the configuration of their browser/e-mail package has not been altered by any computer virus.

Serious breaches of this code may be regarded as gross misconduct and could result in termination of employment. See Disciplinary Action below.

CHAPTER 3 E-MAIL

Where local management policy permits personal use of e-mail, this use should be kept to a minimum and such e-mails should only contain text. Sending graphics and other large file attachments is not permitted where personal e-mail is being sent.

All external e-mail should correctly identify the issuing company and include the details found on that company's letter headed paper.

Nothing should be included in e-mail or other electronic messages that if used in evidence in a court of law, or otherwise made public, would expose the Group to legal penalties or bring the name of the Group, any of its subsidiaries, or personnel, into disrepute.

Employees must not initiate or participate in campaigns that deliver large amounts of unsolicited e-mail to an individual or organisation, (spamming).

Copies of e-mail messages, (Cc: copies) should only be sent where strictly necessary.

Large volumes of e-mail should not be stored on the Group's e-mail servers. This storage is costly and can have a detrimental effect on the performance of the e-mail system. If electronic storage is necessary, this should be achieved using personal folders on the individual's PC.

Where permitted by law, Falcon FoodService reserves the right to scan e-mail for: computer viruses, content that could damage its business and content that is either pornographic or inappropriate and/or prohibited under the terms of this policy document.

The Group also reserves the right to bar access to and from any and all e-mail addresses that it deems should be so barred.

CHAPTER 4 WORLD WIDE WEB AND NEWS GROUPS

Where local management policy permits personal use of the World Wide Web or News Groups, this use should be kept to a minimum. Downloading graphics and other large files that bring no benefit to the business is not permitted.

Employees should pay due attention to maintaining a balance between the amount of time they spend using the Internet and the benefit that accrues to the company through that use.

The company reserves the right to log the details of all Internet sites visited by employees using the computers and Internet connections that it provides and to examine these logs regularly.

Where permitted by law, Falcon FoodService reserves the right to scan World Wide Web pages and News Group postings for: computer viruses, content that could damage its business and content that is either pornographic or inappropriate and/or prohibited under the terms of this policy document.

- Falcon FoodService also reserves the right to bar access to any and all World Wide Web sites or News Groups that the Group deems should be so barred.

The practice of "squatting" registering competitors, brand, or company names as Internet domains to prevent their being used by those competitors, is prohibited. No responsible business should use such tactics and the courts are likely to force the registering business to hand over the domain to a user with a proper claim to it.

CHAPTER 5 LEGAL CONSIDERATIONS

Be careful not to enter contractual agreements or make statements that may be interpreted as contractual unless you intend to. Some communications may need a disclaimer, seek advice from the Group Legal Department in case of doubt. They can advise on suitable wording for such a disclaimer.

- All Internet use must follow laws and regulations, including those:
  - Governing the import and export of technology, software and data;
  - Restricting the use of telecommunications technology and encryption;
  - Governing the transmission of personal data across national borders.

- All Internet use must follow all copyright laws.

- All Internet use must not be harassing, libellous, or disruptive to others' operations.

The Internet provides staff with opportunities to download data or software which may be subject to copyright, often under US law. Staff using software or data from the Internet must

at all times be aware of and respect such third party copyright and any contractual restrictions and company rules of which they should be aware. Those who breach copyright may be liable for prosecution - both the company and the staff - and may also be subject to internal company disciplinary procedures.

Employees should not assume that just because something is available from the Internet, a bulletin board or a network that it is free of any copyright or licence restrictions. One of the many legal problems is that the software licence will be governed by the law of the supplier's country and not the law of the country in which the software is used. This will involve a tangible risk of any company being subject to a number of jurisdictions, many unknown and not well developed.

Downloading of data - the contents of any computer database can be downloaded for storage only with the agreement of the copyright owner. The agreement will normally specify the extent to which data can be downloaded. Further transmission of data from a database via telecommunication system (even within a company's premises) is prohibited unless permission has been received from the copyright owner expressly authorising the licensee to do so.

When putting any information about Falcon FoodService, AFG, or any of its companies or products/services on the Internet, be aware of the requirements of the Trade Descriptions Act in the UK and similar legislation regarding claims for product performance etc. in other jurisdictions.

When using encryption software users must ensure that the laws of all relevant countries are complied with. Some countries, e.g. France and the USA, place certain restrictions on the use of such software.

CHAPTER 6 DISCIPLINARY ACTION

The following behaviours are examples of actions or activities that can result in disciplinary action. This is not a complete list. Disciplinary action may range from verbal warnings to termination of employment depending on the severity of the action.

- Sending or posting confidential materials outside AFG companies or inside AFG to non-authorised staff.
- Theft or copying electronic files without permission.
- Using Falcon FoodService and/or AFG time and resources for personal gain.
- Intentionally transmitting or receiving inappropriate material.
- Refusing to co-operate with a security investigation.
- Breaching any part of the Internet Access Acceptable Usage Policy as detailed in this document and the AFG Internet Access Acceptable Usage Policy which can be found in the AFG Group Manual of Procedures.