**Procedure**

IT and communication play an essential role in our business.

This policy applies to all members of the Company who use our communications facilities, whether directors or consultants, full or part-time employees, contracted or temporary staff. The parameters and restrictions are outlined below, and you are required to read them carefully. The purpose of this policy is to define acceptable email and internet use within working time and is intended to promote effective communication and working practices.

This policy does not form part of any employee’s contract of employment, and we may amend it at any time.

**General principles**

You must use our information technology and communications facilities sensibly, professionally, lawfully, consistently with your duties and in accordance with this policy and our other rules and procedures.

At all times employees must behave with honesty and integrity and respect the rights and privacy of others in relation to electronic communication and information.

Every employee will be given access to the intranet and/or internet as appropriate to their job needs. For those who do not have daily PC access occasional access will be arranged as necessary, by management.

All PC/network access will be through passwords, and no individual is permitted onto the system using another employee’s password. Employees are not permitted to share their password with anyone inside or outside the Company. Individuals will be allowed to set their own passwords and must change them as frequently as requested by the system set-up requirements.  If you are away from your desk, you should log out of or lock your computer.

All information relating to our franchisees and our business operations is confidential. You must treat our paper-based and electronic information with utmost care.

Many aspects of communication are protected by intellectual property rights which can be infringed in a number of ways.  Downloading, copying, possessing and distributing material from the internet may be an infringement of copyright or of other intellectual property rights.

Particular care must be taken when using e-mail as a means of communication because all expressions of fact, intention and opinion in an e-mail may bind you and/or the Company and can be produced in court in the same way as other kinds of written statements.  You are reminded that emails can be used in legal proceedings and that even deleted emails may remain on the system and be capable of being retrieved.

Breach of this policy may be dealt with under our Disciplinary Procedure and, in serious cases, may be treated as gross misconduct leading to summary dismissal.

**Email**

When using your Company email account, you must adopt a professional tone and observe appropriate etiquette when communicating with third parties.

You must not send abusive, obscene, discriminatory, racist, harassing, derogatory, defamatory, pornographic or other inappropriate emails.  We recommend not sending, forwarding or receiving private emails at work which you would not want a third party to read.

Please also refrain from sending or forwarding chain mail, junk mail, cartoons, jokes or gossip.

You must not send messages from another person’s email address (unless expressly authorised) or under an assumed name.

**Email use for personal purposes**

Although our email facilities are provided for the purposes of our business, we accept that you may occasionally want to use them for your own personal purposes.  Personal use is a privilege and not a right.  It must not be overused or abused, and the Company may withdraw permission for it at any time or restrict access at our discretion.

Employees’ work email addresses should not be used to send personal emails and personal email accounts should only be accessed during break times. This is permitted on condition that all the procedures and rules set out in this policy, and the Company’s code of conduct, are complied with.

You must not use your own personal email account to send or receive emails for the purpose of our business.

**Using the Internet**

Internet access is provided primarily for business purposes.  Occasional personal use may be permitted as outlined below.

You are not permitted to access any webpage or download any image or other file from the internet which could be regarded as illegal, offensive, discriminatory, in bad taste or immoral.  As a general rule, viewing a webpage will breach this policy if:

any person (whether intended to view the webpage or not) might be offended by its contents; or

the fact that our software has accessed the webpage or file might be a source of embarrassment if made public.

The Company may block or restrict access to some websites at our discretion.

**Internet use for personal purposes**

Employees should not use the internet during work time for personal use unless in the case of an urgent matter when you should seek the approval of your line manager before use.  Personal use is a privilege and not a right.  It must not be overused or abused, and the Company may withdraw permission for it at any time or restrict access at our discretion.

Employees may use the internet during break times. This is permitted on condition that all the procedures and rules set out in this policy are complied with.

**Unauthorised use of email and internet**

The Company will not tolerate use of email and internet for unofficial or inappropriate purposes.  Examples of unauthorised use include but are not limited to:

any messages that could constitute bullying, harassment or other detriment;

accessing social networking sites such as Facebook, Twitter or Instagram using Company equipment or during work time;

online gambling;

accessing or transmitting pornography;

accessing other offensive, obscene, criminal, or otherwise unacceptable material;

a false and defamatory statement about any person or organisation;

transmitting copyright information and/or any software available to the user;

posting confidential information about other employees, the Company or its franchisees, suppliers, clients, or customers;

any other statement which is likely to create any criminal or civil liability (for you or us); and

any music or video files or other material in breach of copyright.

Instances of misuse or excessive personal use of our systems or inappropriate use of the internet will be dealt with under our Disciplinary Procedure.  Misuse of the internet can, in some cases, be a criminal offence.  In some cases, misuse under this policy will be treated very seriously and can result in summary dismissal.

**Downloading of material**

In order to prevent the introduction of virus contamination into the software system the following must be observed:

unauthorised software including public domain software, magazine cover disks/CDs or Internet downloads must not be used and

all software must be virus checkedusing standard testing procedures before being used.

**Online blogs**

It is not permitted for employees to contribute to online blogs during working hours or using a computer belonging to the organisation. The following rules apply:

personal blogs should contain a disclaimer that the views expressed on it are personal views of the author only;

you should not at any time make comments in a blog which bring the Company into disrepute;

you should not reveal confidential Company information, or information on franchisees/suppliers, customers, clients, employees or any of our staff; etc

you should not at any time make comments in a blog which amount to bullying, harassment are discriminatory or provide any other detriment towards other employees/contractors/suppliers/franchisees or any other individual working in connection with us.

**Storage of emails**

Employees should ensure they regularly audit their emails in order to archive or delete those that contain information that is no longer required in order for the Company to comply with its obligations under current data protection legislation.

**Company’s website**

Unless you are responsible for the upkeep of the Company’s website as part of your role, you are not permitted to add anything to the website without express permission of a line manager.

**Social media**

We operate a social media policy to govern the use of this media within the Company. The policy covers profile pages and other resources maintained by employees on all social networking sites including, but not limited to, Facebook, Twitter, Instagram, and LinkedIn, as well as blogs, forums, message boards, review sites and online polls.  This policy is in place to minimise the risks to our business through the use of social media.  This policy does not form part of any employee’s contract of employment and we may amend it at any time.

Social media can be a distracting technology which causes a negative effect on the productivity of employees working for the Company, however, it can also be an engaging platform that enables the Company to build new relationships with new and existing customers.

This policy sets out how employees must behave when using the Company’s social media platforms and governs how employees should refer to and promote the Company on their own personal accounts.

Social media can involve communication between job applicants and employees and is an avenue for the Company to promote and control their reputation. Social media may blur the boundaries between what is home and work. Access is often public, even amongst a limited group of connected accounts, and comments are often permanent.

Employees should be honest and respectful when using social media. Everything posted on social media may be tracked back to the source so employees must ensure content posted on social media accounts, both in a work and personal capacity, fits with the Company ethos, CSR and marketing brands.

**Terms of use**

Social media usage for work purposes is controlled by the marketing co-ordinator. Approval will be granted by the marketing co-ordinator where use is required for your job role.  You must not express opinions on our behalf via social media unless expressly authorised to do so by the Marketing Director.

Social media usage for personal reasons does not need approval by the Company though you must avoid making any communications that could damage our business interests or reputation.  You should make it clear in social media posts or on your personal profile that you are speaking on your own behalf.  If you disclose your affiliation with us on your profile or in any social media posts, you must state that your views do not represent those of your employer (unless you are authorised to speak on our behalf, as outlined above).  You should also ensure that your profile and any content you post is consistent with the professional image you present to clients and colleagues.

When using social media, either in a personal or work capacity, during or outside working hours, posts on social media must not:

compromise the Company, disclose confidential data or disclose sensitive data;

must not damage the Company’s reputation or brand by defaming or disparaging us, our staff or any third party;

must not breach copyright or data protection;

contain libel or defamatory content;

must not engage in bullying or harassment or any other unlawful discrimination;

be of illegal, sexual or offensive content;

make false or misleading statements;

impersonate colleagues or third parties;

interfere with your work commitments; or

use the name of the Company to promote products or political opinions.

Employees should ensure they consider the Company’s other policies on marketing, promotion, sales and branding.

Social media content attributable to you which breaches the terms of this policy, or the other related policies, may result in an investigation and disciplinary action under the Company’s disciplinary policy.  You may be required to remove any social media content that we consider breaches this policy.  Failure to comply with such a request may result in disciplinary action.

**Business contacts**

Details of business contacts obtained during the course of an employee’s employment are considered confidential information and remain the property of the Company. Business contact details includes the contacts records in computer software installed on an employee’s computer as well as maintained in third party websites including social media.

Business contacts may not be added to personal social media accounts during the course of your employment. If any are, these must be removed upon termination of your employment.

Business contacts may be added to corporate social media accounts. A separate record of business contacts on social media should be maintained within the Company and updated as and when the contacts are added.

**Policy enforcement**

Using social media to refer the Company’s business or personal contacts to an employee’s new employer will be seen as an attempt to solicit customers or poach staff and may result in civil proceedings being brought against the individual.

Using social media in a way which breaches this policy will result in such content being removed from corporate accounts and the employee’s authorisation to use corporate social media accounts on behalf of the Company being suspended and removed. Such content may be damaging to the Company or employees and may lead to disciplinary action under the Company’s disciplinary policy, which may be serious or gross misconduct.

The Company reserves the right to check the social media accounts of employees in accordance with the internet and monitoring policy.

**Monitoring**

The Company is responsible for all business communications but subject to that will, so far as possible and appropriate, respect your privacy and autonomy.  The Company may monitor your business communications for business reasons. ￼

**Enforcement**

Failure to comply with this policy may result in disciplinary action being taken against you. If there is anything in this policy that you do not understand, please discuss it with a member of management.

 **Further Guidance**

**www.acas.org.uk/archive/social-media-in-the-workplace**