Email, Internet, Social Media and Telephone Use Policy

Overview

All employees are encouraged to use email, internet, telephone, and mobiles at work as a fast and reliable method of communication. However, they need to be careful not to expose both themselves and the Company to certain risks and offences that the misuse of these facilities can cause.

All employees have a responsibility to use these resources in a professional and lawful manner and to ensure that they do so in a safe and efficient manner.

IT and communication plays an essential role in the conduct of our business. The IT infrastructure including e-mail and internet access have therefore significantly improved business operations and efficiencies.

This policy applies to all members of the Company who use our or our clients' communications facilities, whether Directors/Consultants, full or part-time employees, contract staff 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.

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 other Company 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 for their 365 accounts (individual log on passwords or Pins for laptop/PC must recorded centrally in case the unit needs to be used while you are absent) and must change them as frequently as requested by the system set-up requirements.

All information relating to our clients/customers 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.

Email Use for Personal Purposes

The Company email facility is provided for business purposes only. Employees must not use the Company email for personal usage whatsoever. Employees should also tell personal email contacts never to send personal emails to them at work.

The content of any email message sent must be neither defamatory, abusive nor illegal and must be in line with the Company's Equal Opportunities Policy. Sending and receiving of obscene or pornographic or other offensive material is not only considered to be gross misconduct but may also constitute a criminal offence.

Employees must ensure that they have the correct email address for the intended recipients. If employees inadvertently misdirect an email, they should contact their manager and the Data Protection Officer (DPO) immediately on becoming aware of their mistake.

Employees must not send any information that the Company considers to be confidential or sensitive over the email.

In this policy, "Confidential Information" refers to any material belonging to the Company which is confidential in nature, concerns trade secrets or other confidential data of the Company or its customers or clients.

Confidential Information must never be transmitted or forwarded to third parties who are not authorised to receive it.

Internet Use for Personal Purposes

Employees are not permitted to use the internet during work time unless in the case of an urgent matter when you should seek the approval of your line manager before use.

Employees may use the internet during break times and must not exceed 30 minutes per day. 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.

Unauthorised, excessive or inappropriate use of the internet for non-work related purposes may render the employee liable to disciplinary action.

Unauthorised Use of Email and Internet

The Company will not tolerate use of email and internet for unofficial or inappropriate purposes, including:

- any messages that could constitute bullying, harassment or other detriment
- accessing social networking sites such as Facebook using Company equipment or during work time
- on-line gambling
- accessing or transmitting pornography
- accessing other offensive, obscene or otherwise unacceptable material
- transmitting copyright information and/or any software available to the user
- posting confidential information about other employees, the Company or its customers or suppliers.

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/World Wide Web downloads must not be used
- all software must be virus checked by the Data Protection Officer (DPO) using standard testing procedures before being used
- permission should be sought before downloading any programme or app that is not preloaded on the IT you use.

On-line Blogs

It is not permitted for employees to contribute to on-line 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 clients/customers/suppliers etc
- you should not at any time make comments in a blog which amount to bullying, harassment or any other detriment towards other employees/ contractors/suppliers/clients/customers 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 the GDPR Regulations 2018 and the Data protection Act 2018

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 manager.

Monitoring

The Company is ultimately 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.

Social Media

The Company operates 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 networking sites including, but not limited to, Facebook, Twitter, Instagram and LinkedIn, as well as blogs, forums, message boards, review sites and online polls.

The use of social media can be an engaging platform that enables the Company to build new relationships and engage with new and existing customers and it is important that employees using social media in the workplace use it in a way which does not adversely affect the Company's reputation.

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
- must not breach copyright or data protection
- contain libel or defamatory content
- must not engage in bullying or harassment
- be of illegal, sexual or offensive content
- interfere with your work commitments
- use the name of the Company to promote products or political opinions.

The Company reserves the right to review and monitor your personal activity, participation or comments on social media networking sites where the Company has a reasonable suspicion that you 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.

Making Personal Telephone Calls During Work Hours

Company phones, landline and mobile, are primarily for work purposes and for calls of a business nature.

Permission to make personal calls during working time can be obtained from the employee's line manager. Personal calls should be brief and made on a one-off basis. There should not be a regular stream of requests for personal calls to an employee's line manager.

Personal mobile phones should only be used on an employee's break or lunch hour and should not be used during working time.

Personal mobiles can be on vibrate for emergency calls only, replies to texts or calls can only be made during breaks.

To secure the effective use of the Company telephony infrastructure and to ensure there is no unauthorised or excessive usage of Company phones for personal calls, there will be regular monitoring undertaken and reporting conducted on the usage of the Company phone system. This may lead to monitoring of an individual employee's usage of the Company telephony infrastructure, if excessive use is detected. All data processing undertaken by monitoring in this way will be done in accordance with the General Data Protection Regulation and Data Protection Act. We rely on the lawful basis of legitimate interests to undertake such processing. The Company's privacy notice provides more information on the personal data we use and how we use it.

Enforcement

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