IT, E Mail & Internet Usage Policy

This policy applies to all companies within the Relyon Group.

The computer systems of the Company represent the heart of our ability to provide services to our clients. Protecting them is essential for the business to succeed. Therefore, the Company will take all the steps necessary to safeguard these systems and each employee should see it as a fundamental part of their job to help. This includes avoiding risks such as introducing unauthorised software, complying with copyright and Data Protection law, and being careful to protect the security of sensitive information.

This document outlines the procedures and employee responsibilities when accessing the Internet, sending & receiving emails and using the company's computer systems.

The Company views misuse of computers as misconduct which could, depending on the circumstances, result in dismissal.

Misuse amounting to criminal conduct will be reported to the relevant authorities.

Ownership

Only Company approved and licensed software, and approved data are allowed on the Company's computers. Removal of all unauthorised software is required. If unauthorised software is found on a system, the software will be deleted immediately and without question, including all associated data files.

Internet access and email equipment are the property of the Company.

Email messages that are created, sent or received using the Company equipment are the property of the Company

The Company reserves the right to record and disclose all web sites visited using its equipment.

General

Employees are only allowed access to those parts of the computer system which they need to carry out their normal duties.

Employees must comply with local procedures to ensure that all software introduced is virus-free.

Should employees have access to personal data, they must bear in mind at all times the provisions of the Data Protection Act.

Employees must observe the Computer Misuse Act 1990, in connection with both the Firm and third parties.

Passwords must be used at all times and changed regularly; avoidance of obvious passwords is recommended.

Passwords should be a minimum of twelve characters.

Employees are responsible for the security of their own passwords and workstations.

Employees must not purchase, install or use unlicensed software on Company or customer equipment.

Computer game playing is not permitted whilst in a work environment.

The downloading, transmission or storage (including streaming) of music or video for personal use in strictly prohibited.

Use of any Company systems including email and the internet to conduct private or freelance business for the purpose of commercial gain is never acceptable.

To ensure compliance with this policy and the attainments of the policy objectives both private and business use of e-mail may be subject to monitoring.

Email

E mail Conduct – General

Employees may use the e-mail system for modest personal use outside working hours, however it should be kept to a reasonable level. Inappropriate or excessive use of the email system for personal reasons may result in disciplinary action and/or removal of the facility.

Global or site e-mails should not be used for personal issues which are non work related at any time.

The Company retains the right of access to and ownership of all email sent from and received by its systems.

E-mail is an excellent tool for imparting information in an informal and friendly manner. However because of the relative informality of email it is sometimes used without due consideration as to how it will be received.

Never send an email in haste or anger – once the 'send' button has been pressed an employee will not be able to stop the message being received.

E-mail messages should be treated as permanent written records which may be read by other people and which could result in personal or Company liability

The points below should help you in making the decision to send.

Before sending an email you should consider:

If the content and the purpose of the e-mail is really necessary. Face to face talking is always the best option if there is a problem to resolve.

Email should not be used as a substitute for interaction with colleagues.

The content and tone of the email. Do not type anything would not be acceptable to say directly to the recipient in person. E-mail is faceless and can be misinterpreted.

If the message may contain content that may be considered illegal, offensive or disruptive

The ease and speed of e-mail can lead to inadequate thought going into a message, and the possibility of the words or tone being misinterpreted by the recipient.

Abrupt, inappropriate and unthinking use of language can lead to a bullying tone and possible offence to others, even harassment, for example, capitals are often interpreted as shouting.

Employees should not:

Assume because an email has been sent that they are absolved from responsibility for resolving the problem and further action is unnecessary.

Retrieve or read email messages that were not sent to them unless authorised by the company or by the email recipient.

Impersonate any other person when using email

Amend any received emails prior to storing, printing or forwarding them.

Use email to send defamatory messages that criticise other individuals or organisations.

Send or distribute e-mail messages which are abusive, defamatory, pornographic in nature or make any improper or discriminatory reference to a person.

Copy, download or forward to third parties, via e-mail, the work of other people protected under copyright, without their consent.

Remove or change the email disclaimer that is automatically attached to all outgoing messages.

Enter into contractual commitments by email

Create email congestion by sending trivial messages. It is strictly forbidden for anyone to copy/forward e mails such as chain mail letters, humorous stories, etc., or large attachments.

Send bank account or credit card information over the Internet.

Before using the CC Function Employees should:

Consider who really needs to receive a copy of an E-mail. Reduce the number of "cc" copies to send on a need to know basis.

Not copy an email as a political statement or to put pressure on the recipient.

Consider address groups set up in your e-mail personal address book. Whilst these are quick way of copying everyone in on the same message, employees should be aware that all recipients of the e-mail are able to see all the other names of those to whom the message was sent. This might not always be desirable – the obvious example is e-mailing a group of customers/clients or suppliers where we don't want to give information about other customers/clients we are dealing with. Using the "blind copy" function is not a solution to this problem, as the server receiving the e-mail may convert into "cc's" and so again all addresses names are displayed. The only solution is to avoid using these address groups (or sending the e-mail to more than one person) when the addressee list sent with the mail could be viewed with interest by one of the receiving parties.

External E mails

All email communication must be handled in the same manner as a letter, fax, memo or other business communication. Employees should not send any information or write in any style that would be inappropriate to write on headed paper as an official company communication.

No copyrighted or company propriety information is to be distributed by company email or via the Internet unless approval has been granted by a company official.

Jokes sent via Email

It takes only seconds for a joke to be circulated by email. What may be amusing for one employee could be insulting to another.

Email communications are capable of amounting to harassment giving rise to a claim of discrimination on the grounds of sex, race (nationality), religious belief, sexual orientation, age or disability. In these circumstances a claim could be made against the individual who sent or forwarded the email and against the Company.

It is unacceptable to use email to circulate discriminatory or harassing statements. Should emails be circulated with content which could or does cause offence to any individual the disciplinary procedure will be invoked and such action may be consider gross misconduct.

Non-Business Email

Incidental and occasional personal use of email is permitted. Such messages become the property of the company and are subject to the same conditions as company email messages.

Virus checking of email attachments

Virus checking software is pre-loaded on all computer equipment provided by the Company, this in turn will automatically check and, where possible, repair or delete any file attached to an email message that contains a computer virus.

However, due to the constant creation of viruses by parties outside the control of the company, it is the responsibility of the employee to inform the appropriate Company official of any emails received (with file attachments) sent by an unknown and/or untrusted source prior to opening the file attachment.

It is also the responsibility of the recipient to ensure email attachments seem reasonable before opening them.

The Company reserves the right to block any emails that it deems to break any of the rules above.

Internet Usage

The use of the Internet for personal matters is permitted if the use is incidental, occasional and outside working time. Inappropriate or excessive use of the internet for personal reasons may result in disciplinary action and/or removal of the facility.

Internet sites browsed/visited must not contain content that may be considered illegal, offensive or disruptive.

Offensive content includes but is not limited to pornographic, obscene or harassing language or images, racial, ethnic, sexual or gender specific comments or images, or other comments or images that would offend someone on the basis of their religious or political beliefs, sexual orientation, national origin or age.

An employee must not distribute confidential, proprietary, and/or sensitive corporate information to external Internet sites or users without the appropriate authority.

Accessing or updating social networking sites (e.g. facebook or myspace), chat rooms or online blogs is not acceptable at any time.

The Company retains the right to block access to any Internet site they deem may contain inappropriate material.

External Internet Use

All employees should be conscious at all times of the information they place or way in which they portray the Company in any online forum.

Employees who post information on websites including (but not limited to); social networking sites, online blogs, open chat rooms and discussion groups outside of work, may be subject to disciplinary action and/or dismissal should that posting contain any confidential Company information or have the effect of bringing the Company into disrepute.

Monitoring

The Company recognises that employees have a legitimate expectation that they can keep their personal lives private and that they are also entitled to a degree of privacy in the work environment.

However the Company reserves the right to monitor employee email or internet activity where it is necessary to prevent or detect;

- Unauthorised use of the Company's computer systems
- Any criminal activity including but not limited to fraud, harassment and obscenity
- Any detrimental impact upon the efficient operation of Company systems
- Any breach of regulatory guidelines
- Excessive personal use of the internet or email-system.
- Any breach of this IT, E Mail & Internet Usage Policy or any other of the Company's rules of procedure laid down in the contract of employment or the Company Handbook

All employees are hereby notified that the Company has the ability and legal right to monitor e-mail usage and internet usage. By using e-mail and internet the employee consents to any monitoring the Company considers justified to achieve one of the above aims or to protect any other legitimate interest.

When the monitoring of personal e-mails is necessary monitoring will be confined to the message address or heading.

Covert monitoring will only be performed in exceptional circumstances and only when sanctioned by a senior manager of the company.

If information gathered from monitoring may have an adverse impact on an employee, it will be presented to them and they will be allowed to make representations before any action is taken.

Information gathered through monitoring will only be used for the purpose for which the monitoring was carried out, unless the monitoring leads to the discovery of an activity that no employer could reasonably be expected to ignore.

All information gathered through monitoring will be held securely and kept for no longer than is necessary to achieve the aim for which it was collected.

Disclosure

All employee's are under a duty to report the following to their line manager:

- suspect e mails/e mail attachments
- suspect web sites
- obscene/illegal material found on a PC or sent via email
- persistent use of the internet or e mail system for personal reasons
- persistent downloading of illegal/obscene/offensive material.

Breach of Policy

Staff will be liable to disciplinary action if they are in breach of this IT, E Mail & Internet Usage Policy.

Depending on the severity of the offence staff may be liable to summary dismissal.

If staff conduct and/or actions are unlawful or illegal the individual may be personally liable. Information relating to the commission of a criminal offence may be passed to the relevant prosecuting authority.