1. IT POLICY

Policy

This policy applies to all Roe Group employees incorporating Roe Bros & Co Ltd, North West Steel Ltd, subsidiaries and affiliated companies. It is the responsibility of all operating units to ensure that this policy is clearly communicated, understood and followed.

It is the intent of this policy to establish guidelines for the employees of the Roe Group using the Company's computing facilities, including computer hardware, software, printers, fax machines, voicemail, e-mail and internet facilities (this list may not be exhaustive), collectively called 'Information Technology'.

It is also the intent of this Policy to protect Roe Group employees from any defamatory employee publications, interaction or online representation that references the Company and / or its employees as above, either on the Roe Group information technology or on privately owned information technology.

This Policy is provided to regulate usage and to inform employees of the Roe Group the Company Policy in that respect.

The Roe Group makes computers, internet and e-mail services available to its employees as a tool to help them perform their jobs more efficiently and encourages use of this technology in a professional and reasonable way so that the confidentiality, integrity and availability of the Company information and computing services are neither misrepresented nor prejudiced.

The rules in this Policy are very important and any violation could result in disciplinary action and/or summary dismissal for Gross Misconduct.

A clearly formulated policy can help ensure that decisions made within the Roe Group which affect employees:

- Are well thought out, understood by all users, are consistent and fairly applied
- Take full account of their effect on all areas of activity
- Satisfy legal requirements
- Contribute to a productive relationship between the employer and employees

Purpose

By having a written policy the Roe Group can:

- Help protect itself against liability for the actions of employees (vicarious liability)
- Help educate system users about the legal risks that employees might inadvertently take
- Make clear to employees who they should contact about any particular aspect of the policy
- Notify employees of any privacy expectations in their communications
- Prevent damage to systems
- Avoid or reduce unnecessary time being spent on non-work related activities

Access to the Roe Groups Information Technology is to be used for the Company's legitimate business purposes and for that reason, any violation of any of these rules is considered Gross Misconduct, possibly resulting in summary dismissal.

The Company does permit a limited amount of personal use of these facilities, including computers, printers, e-mail and internet access, which would be before or after your scheduled start and finish times and during your scheduled lunch break, although all employees must use these facilities responsibly and personal use must never interfere with individual work responsibilities, since misuse by even a few individuals has the potential to negatively impact productivity, disrupt company business and interfere with the work and rights of others.

When using the Information Technology of the Roe Group for personal use, only the limited amount of personal time outlined above may be allocated to:

- Writing personal correspondence.
- Sending / receiving personal e-mails
- Accessing the internet for purposes other than Company business

The Roe Group will not permit:

- Playing games
- Participating in chat rooms

- Copying software for personal use
- School-work, papers, novels or any other material that does not relate to your employment
- The printing of non Roe Group documentation without permission
- Using Company accounting programs for personal use
- Using Company software or design programs for personal use
- Downloading, opening or distributing unauthorised software
- Generating or otherwise participating in the distribution of a virus and/or deliberately sending junk e-mail (spam)
- This list is not exhaustive

Unauthorised Software

Software other than that provided by the Company is not to be loaded onto Company computers unless specifically authorised by the IT Manager or Head Office.

Confidentiality of Passwords

Passwords are confidential and must not be given to another person without prior permission from your Depot Manager or Head Office. At the time of preparing to leave the Company you must immediately make any passwords used in the course of your employment known to your Depot Manager and/or Head Office.

All Depot Managers and employees must make passwords known to the Chairman or a Director immediately upon request.

Virus Notification

Notify your Depot Manager immediately if you observe or become aware of a virus or any other program that could damage the computer system.

Any employees who think they have imported a virus onto the system, an e-mail has a suspect attachment or are sent a ‘chain letter’ or any other queries or concerns should contact the Company IT Manager or Head Office without delay.

Generation or Storage of Offensive Material

The use of the Roe Groups computers for the generation or storage of distasteful or offensive material is strictly forbidden ("offensive" means – may cause distress if it is received or discovered).

No Right to Privacy

You have no right to privacy with respect to e-mails received on the Roe Groups computers. Any e-mail processed on Company computers may be subject to scrutiny by Company management at their discretion for the following reasons:

- To establish the existence of facts
- To ensure compliance with regulations
- In the interests of national security
- To prevent or detect crime
- To investigate or detect unauthorised use of the Company telecommunications
- To secure effective system operations
- To determine whether received communications are business or personal communications
- To monitor communications made to anonymous help lines
- This list is not exhaustive

You have no right to privacy with respect to Internet usage. Any internet sites accessed on Company computers may be subject to scrutiny by the installation of computer software to enable Company management to view and monitor employee internet usage.

The Roe Group reserves the right to introduce software for automatic blocking and/or monitoring the flow, content and usage of internet sites. The unauthorised removal of such monitoring software may result in disciplinary action being taken.

Use for Inappropriate Conduct

The Company strictly prohibits the access, viewing, posting, downloading, storing, transmitting, sharing, printing or distribution of any information or material from any source as follows:

- Pornographic
- Profane
- Abusive
- Obscene
- Indecent
- Racist
- Sexist
- Violent Images
- Offensive
- Insulting
- Discriminatory
- Harassing
- Offensive
- Incitement to criminal behaviour
- Otherwise inappropriate in a business environment

Jokes

Using e-mail for the receipt and distribution of jokes and banter is not permitted. E-mail is one of the least secure methods of communication. What may seem a joke to you may be offensive to someone else.

Chain Letters

Use of e-mail to generate, participate or otherwise become involved in e-mail chain letters/messages is forbidden.

Junk Mail (Spam)

Sending and responding to junk e-mail is forbidden

Uploads and Downloads

Uploading, downloading, opening or distributing unauthorised software is forbidden.

Viruses

Generating or participating in the distribution of a virus or any other action that may compromise the security and safe function of the Company systems is forbidden.

Confidential Information

You are responsible for ensuring that you only use e-mail to reproduce, replicate, duplicate or distribute confidential or sensitive Company information to the appropriate party. Negligent distribution of Company information to those for whom it is not intended is a disciplinary office.

Identification

You must always identify yourself in an appropriate manner in any e-mail communication made in the proper course of your employment.

Opinions

You must not express opinions or views that could be interpreted as misrepresenting the Company's products, services, trademarks or those of any other organisation.

Trademarks and Licensing Rights

You must not infringe the trademark and/or licensing rights of the Company or any other organisation.

Good practice procedure

- E-mail is not an informal communication tool, but has the same authority as any other communication to and from the Company therefore all employees should always exercise responsible behaviour
- All e-mails sent on behalf of the Roe Group should have a disclaimer attached
- E-mails should be regarded as published information

- Binding contracts may be inadvertently created, therefore all employees are to act responsibly in all communications entered into and to contact their Depot Manager / Chairman or a Director if further advice/assistance is required
- Check your mailbox daily, more if warranted
- Once read, messages should be either deleted or archived
- If you have arranged for someone else to receive your e-mail, you must have notified that person in advance
- After completing your work on the internet, sign off, unless authorised to be on continuous use
- Do not leave confidential or sensitive information on your computer screen
- Virus check all material received from the internet
- Virus check all material you may pass along

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. In all instances, the Roe Group prohibit inappropriate messages, for instance, any that might cause offence or harassment on grounds of age, sex, race, disability, age, religion (this list is not exhaustive).

All employees are expected to exercise responsible and ethical behaviour when using the Company's Information Technology facilities. Any action that may expose the Company to risks of unauthorized access to data, disclosure of information, legal liability, or potential system failure is prohibited and may result in disciplinary action up to and including termination of employment and/or criminal prosecution.

Blogs, chat rooms, social networking sites

Online social networking opportunities including professional blogs and micro blogs, communities and forums, wikis, peer to peer sharing networks and other channels of online discussion and interactive publishing are increasingly common. These collaborative and interactive resources can profoundly impact the way that the Roe Group employees work, interact and support each other and the organisation. However, interaction with a community outside of the Roe Group and its staff can introduce risks to the Company.

Employees who participate in social networking channels must interact responsibly and avoid actions that undermine productivity, expose proprietary information or violate the privacy of the Roe Group and its employees, customers and suppliers.

This policy respects the right to privacy outside of the workplace, but an employee publication, interaction or online representation that references the Roe Group or its employees in part or at any time is considered to be covered in its entirety by this policy.

The following types of information may not be disclosed without explicit consent of the Roe Group:

- Conversation between employees
- Announcements, documents, discussions or other information shared in internal communications
- The names of clients, partners, suppliers, customers or other employees. It can be acceptable to use a pseudonym as long as this reference does not, by design or inference, reveal the true identity of the referent.
- Internal e-mails, notes, memos or other interpersonal communications
- Internal documentation not specifically marked for external distribution
- Publications or draft documents ultimately intended for public distribution
- Planning documents, production documents or software code
- Organisational charts
- Organisational contracts, policies and other legal documents
- This list is not exhaustive

Personal blogs and websites should not be used to attack or abuse colleagues. Staff members should respect the privacy and feelings of others. If an employee breaks the law on a blog (e.g. by posting something defamatory) they will be personally responsible.

All employees of the Roe Group also agree to comply with applicable country laws, and to refrain from engaging in any activity that would subject the company to any liability.

The Roe Group reserves the right to amend these policies and practices at any time without prior notice and to take further actions as may be necessary or appropriate to comply with Company policy.

To protect the integrity of the Roe Group's computing facilities and its users against unauthorised or improper use of these facilities and to investigate possible use of those facilities in violation of Company rules and policies, the Roe Group reserves the right, without notice, to limit or restrict any individual's use, and to inspect, copy, remove or otherwise alter any data files or system resource which may undermine the authorized use of any computing facility or which is used in violation of Company rules of policies.

The Roe Group also reserves the right to periodically examine any system and other usage and authorisation history as necessary to protect its computing facilities. The Roe Group disclaims any responsibility for loss of data or interference with files resulting from its efforts to maintain the privacy and security of those computing facilities or from system malfunction or any other cause.

Scope

This policy covers the usage of all the Company's Information Technology and communication resources, including, but not limited to:

All computer related and similar equipment including desk top personal computers, (PC's), laptops, terminals, PDA's, wireless computing devices, telecom equipment, mobile phones, networks, databases, printers, servers and shared computers and all networks and hardware to which this equipment is connected.

All software including purchased or licensed business software applications, Company written applications, employee of vendor/supplier, written application, computer operating systems, firmware and any other software residing on company owned equipment.

All intellectual property and other data stored on company equipment.

All of the above are included whether they are owned or leased by the company or are under the company's possession, custody or control.

This Policy also applies to all users, whether on Company property, connected from remote via any networked connection or using Company equipment or privately owned information technology where employees are

making specific reference to the Roe Group, , Roe Bros & Co Ltd, North West Steel Ltd, subsidiaries and affiliated companies and also its employees.

Monitoring

Use of our computers and IT systems (including internet and email) are monitored. This also includes personal use of them. Monitoring is carried out lawfully and to the extent that it is necessary for business purposes. To ensure monitoring is justified, the Company has carried out an impact assessment.

The Company reserves the right to carry out monitoring for the following (non-exhaustive) purposes:

- To prevent or detect crime;
- To comply with any legal obligations;
- To monitor compliance with this policy;
- To ensure compliance with company procedure;
- To monitor the quality of work;
- To investigate alleged or suspected wrongful acts;
- To secure effective system operation.

Monitoring may be carried out producing a report for usage. Monitoring reports detail personal and business usage highlighting any areas of concern. Only senior management will have access to reports produced. Monitoring of emails is usually confined to address or heading, unless it is necessary for good reason to access the content. Senior management have authority to carry out monitoring. Data will be protected by appropriate measures.

Information obtained by monitoring may be used as part of disciplinary, capability or other Company procedures set out in this handbook. This may involve the examination and disclosure of information obtained by monitoring to persons involved in any applicable procedure (where appropriate), including those nominated to undertake an investigation and any witness, manager, director and/or chairperson. If necessary information obtained by monitoring may be handed to the police in connection with a criminal investigation. Serious violation of this policy may result in summary dismissal for gross misconduct. This is the case whether or not the breach takes place during or outside working hours and whether or not you used company systems or computers.