Policy Overview

This policy describes the guidelines of the Company with regards to the use of its IT & Communication equipment and disclosure of e-mail messages sent or received. This policy applies to all employees of James Fisher & Sons plc as well as to any contractors / agency workers that use the Company's IT & communications equipment including computers, telephones, WI-FI and network.

Introduction & General Principles

Whilst the Company encourages employees to embrace the use of its IT resources to its fullest extent it is important that guidelines are issued for the protection of the individual and the Company.

There are common sense guidelines for the way in which employees are expected to conduct themselves from day to day whilst at work. It should be noted that:
e-mail

- The Company provides employees IT equipment to use to its fullest extent to ensure we work at our fullest and most effective capacity.
- The Company demands respect from all employees for its clients, Directors, the wider community and for each other. This means IT & communication systems must not be used in a detrimental or offensive way.
- The Company demands integrity from all employees so that we are confident that the Company is not or cannot be accused of facilitating any unlawful or offensive action at any time.

The Company respects the individual privacy of its employees. However, employee privacy does not extend to the employee's work-related activities or to the use of Company provided equipment or network / internet access. Employees should be aware that this policy might affect their privacy in the workplace.

Use of Company Telephones (including Mobile Phones)

In line with their role, employees are permitted to make occasional private telephone calls during their scheduled breaks or outside working hours. The timing of personal calls should, wherever possible, cause minimal disruption to the employee's work.

Employees should refrain from making calls to premium rate numbers and international calls except in circumstances that is related to their day to day responsibilities as part of their role within the Company. The same principles apply to text and picture messages.

Where a mobile phone has been issued by the Company to the employee, it will remain the property of the Company. The employee will be responsible for its safekeeping, proper use, condition and eventual return to the Company.

The use of the internet & e-mail access on Company mobile phones is allowed where the employee has been allocated a suitable data tariff on their mobile phone plan. It is the employee's responsibility to use data responsibly & within the data tariff limits.

Employees must ensure that their mobile phone is protected by a Personal Identification Number & this must not be disclosed to anyone.

Company Mobile Phone Use Outside of UK

The employee must ensure that "data roaming" is switched off for any times other than checking Company e-mails. "Data roaming" outside the UK can result in very high charges, and if it is found that these have been incurred due to personal use or negligence on the part of the user, then the charges may be passed on to the user. It is the responsibility of the employee to ensure they are on the appropriate tariff when travelling outside the UK.

Use of Personal Mobile Phone

The Company does not operate a Bring Your Own Device (BYOD) policy. If an employee uses a personal phone to access Company Email or other Company Applications, then they must inform GBS if the phone is lost. All data on that phone may then be remotely deleted. Users must ensure their mobile phone as a minimum is protected by a Personal Identification Number (PIN).

Using Mobile Phones Whilst Driving

It is an offence to use hand held mobile phones or similar device whilst driving or whilst the engine is turned on

Internet & E-mail Access

As a condition of providing internet / e-mail access to its employees the Company places certain restrictions on workplace use of the Internet and e-mail, the system must be used for the following :-

- To communicate with fellow employees and clients regarding matters within an employees assigned duties
- To acquire information related to or designed to assist and/or improve the performance of the job holder
- To facilitate performance of any task or project in a manner approved by the Company

Compliance with Applicable Laws and Licences

Employees must comply with all software licences, copyrights, and all other laws governing intellectual property and online activity. Employees are also reminded that installation of any software onto the computer systems must have approval beforehand. If in doubt, please contact Group Business Systems Department for guidance.

The Data Protection Act applies to e-mail as it does to all forms of stored information. This means that employees must ensure that an e-mail containing personal data:

- is not disclosed to unauthorised persons
- is only kept if it is required for our work, and
- is kept secure at your place of work including printouts.

Only keep e-mail which needs to be kept. Users are responsible for managing their own records e.g. filing records in an appropriate and organised manner.

Personal Use of E-mail & Internet

Because the Company provides e-mail and internet to assist employees in the performance of their job, employees should use it primarily for business use. Incidental and occasional personal use is permitted provided it is not excessive and does not interfere with the proper performance of the employee's duties.

The Company may withdraw permission for personal use in individual cases in which an employee is found to be abusing the facilities.

Misuse of E-mails or Internet

Please note that employee use of e-mails and internet provided by the Company expressly prohibits the following in or outside of Company time:-

- Intentional distribution of destructive programs (i.e. viruses and/or self-replicating code)
- Intentional damage or interference with other systems
- Access to, use of and / or distribution of obscene files
- Dissemination or printing of copyrighted materials (including articles and software) in violation of copyright laws
- Sending, printing or otherwise disseminating proprietary data, trade secrets or other confidential information of the practice or its clients in violation of Company policy
- Sending, forwarding or distributing e-mails / messages containing offensive or harassing statements, images or language likely to intimidate, threaten or in any way cause offence to others based on their race, national origin, sex, sexual orientation, age, disability, religious or political beliefs or personal characteristics
- Sending or soliciting sexually orientated messages or images
- Operating a business in direct conflict to the Company's services or products or any form of soliciting money for personal gain
- Sending chain letters, gambling or engaging in any other activity in violation of the law
- Usage that has a detrimental impact on the Company's network performance. For example, watching videos, downloading large files from the internet that are non-work related

The above list is not exhaustive and employees should be aware that a degree of common sense is required when using the Company's IT & communication systems.

Consequences of Misuse

Violation of the Company's policy may result in disciplinary action. The measure of discipline will correspond to the gravity of the offence as weighed by its potential effect on the Company and fellow employees.

Security

Access to the Company's computers requires a system enforced complex password. Under no circumstances should an employee disclose their password or record it in a place where it can be viewed or readily accessed. In the event that an employee needs to allow another employee to access their e-mail, this can be arranged without disclosing details of their password (Group Business Systems can assist with this). Should an employee find that their password has been compromised, it is the responsibility of the employee in the first instance to change their password using the self-service functionality.

Employees should protect the security of their terminal by ensuring they lock their terminal when leaving their workstation and log out at all times when leaving the office (unless advised not to do so by Group Business Systems).

Employees should also be aware that e-mails are not a secure way of sending information. Employees are encouraged to take extra care when sending sensitive information (e.g. password protection).

Employees should not install or re-configure any network equipment unless under the guidance of Group Business Systems – this includes equipment such as routers, Wi-Fi Access Points etc.

Virus Detection

Although the Company has installed virus software, this does not guard against all viruses. Employees should take care when opening e-mails and attachments especially when from unknown sources. The Company computers are configured so USB devices do not auto-run programs. Users must exercise caution when opting to run programs from a USB device.

Employees should refrain from using unlicensed software and should seek permission of Group Business Systems before installing any software onto Company computers/communication systems.

WIFI

The Company may have wireless facilities on site for the use of employees and clients. Use of the Company Wi-Fi will be monitored and the same principles outlined in this policy will apply in using the Company Wi-Fi.

Monitoring of IT & Communication Systems

Employees must be aware that when using the Company's communication systems, the contents of e-mail communications / internet usage / phone records are accessible at all times by the management / Group Business Systems. The use of the system will imply consent to search. This includes the use of personal devices using Company communication systems.

The Company reserves the right to monitor e-mails / internet / phone /mobile usage and will exercise the right in order to:

- Ensure the effective operation of the Company's telecommunications systems and to maintain security,
- Investigate and detect unauthorised use of the systems in breach of Company policies, such as excessive personal use or distribution of inappropriate material,
- Monitor standards of performance
- Check whether matters need to be dealt with in an employee's absence
- Investigate allegations of misconduct, breach of contract, a criminal offence or fraud by the user or a third party
- Pursue any other legitimate reason relating to the operation of the business.

Loss / Theft / Damage to Company Property

If an employee's Company mobile phone or computer (or any associated accessory) is lost, stolen, damaged as a result of careless, negligence or vandalism, the employee may be required to reimburse the Company for the cost of repair/replacement. Any employee who fails to reimburse the Company (in full or in part) will have the appropriate amount deducted from his / her pay.

If an employee leaves the Company's employment (for any reason) and fails to return his / her Company property, s/he will have the appropriate amount deducted from his / her final pay. If this is not possible, the Company will take appropriate action against the employee to recover the equipment or compensation for loss.

The user is responsible at all times for the security of their mobile phone and it should never be left unattended in a public place. A PIN number should be used on the mobile.

If the mobile phone is lost or stolen, this must be reported to our mobile phone partner, CommTech on 01603 218600

Further Information & Guidance

This policy should be read in conjunction with the other Group Employee Handbook and specifically the Social Media Policy.

Scope

- This policy applies to all business units of James Fisher Group and other associated workers.
- This policy is for guidance only and does not form part of your contract of employment.