

Use of Company Facilities Policy

*(Email, Acceptable Internet Usage / Company
Documentation & Telephones)*

Contents

1. Introduction.....	2
2. Company Policy	2
3. General Procedures	2
4. Viruses	2
5. Access & Remote Access	2
6. Prohibited Uses	3
7. Security.....	3
8. Monitoring.....	4
9. Contracts	4
10. Confidentiality	4
11. Copy Right.....	4
12. Personal Use	4
13. Company Telephones.....	5
14. Disciplinary	5

1. Introduction

This company views email and the use of the internet as an important business tool. It is therefore important that we have in place a policy to protect the quality and integrity of all of the company's electronic communications and to provide employees with standards of behaviour when using them.

This Policy sets out guidelines for managing electronic documentation, the use of email and internet use by all employees to encourage them to use email and the internet in the business environment in the correct manner. Any breach of this policy or misuse of electronic communications may constitute a serious disciplinary matter and may lead to disciplinary action and in severe cases to dismissal.

2. Company Policy

It is the policy of the company to encourage the use of its electronic mail and internet services to share information, to improve communication. However, we must prohibit any unauthorised and improper use of these means of communication. All staff must comply with the Computer Misuse Act <https://www.legislation.gov.uk/ukpga/1990/18/data.pdf> which protects data held by organisations from unauthorised access and modification.

Use of the email and internet facilities is permitted and encouraged in circumstance where the use is suitable for business purposes and supports the goals and objectives of the company and is to be used in a manner that is consistent with the company's standards of business conduct and as part of the normal execution of an employee's job responsibilities.

Those who use the company email and internet services are expected to do so using responsibility and must comply with this and all aspects of the company's Email and Internet Policy. Personal use of email internet facilities is restricted to the terms of "clause 9".

3. General Procedures

The following procedures apply to all electronic communications sent by employees and all use of the internet if using the company's access accounts or equipment. It also applies to employee's use of their own access accounts accessed via the company's equipment or accessing the company's network by an employee's own equipment.

4. Viruses

All computers should use authorised and current anti-virus protection software. No unauthorised anti-virus software should be installed, transmitted or downloaded.

5. Access & Remote Access

The company's computer equipment and systems must only be accessed and operated by those authorised to do so. Unauthorised use, intentional interference with the normal operation of the network or failure to comply with this policy will be regarded as gross misconduct and may lead to dismissal and possible criminal prosecution.

The company reserves the right to designate those employees to whom it will provide access to the internet and electronic mail services and may revoke access at any time to persons without giving reasons for doing so. Internet access is controlled by the company and the

company reserves the right to prevent access to any sites it deems unacceptable. Any employee attempting to evade the controls instituted will be suitably disciplined and may be dismissed in appropriate circumstances.

Remote access to the company's network will be at the discretion of 'The Company' and may be revoked at any time. Documentation must not, under any circumstances be removed and held on any employee's personal computer or storage device (e.g. memory sticks, CD, MP3 players etc) without the express permission of a member of the Board. All computers being used for remote access should use authorised and current anti-virus protection software.

6. Prohibited Uses

- Employees must not view, store, transmit, upload, download or intentionally receive communications, web pages, files or documents that are or could be interpreted as intimidating, harassing or illegal or containing hostile, degrading, sexually explicit, pornographic, discriminatory or otherwise offensive material.
- Employees must not send unsolicited emails, or email messages to multiple recipients nor use email for personal gain nor represent personal opinions as those of the company.

7. Security

- All software downloaded to a company computer must be approved by a member of staff responsible for IT systems before installation to assure compatibility with software already installed on the computer. Problems may arise when unauthorised software is installed which is not compatible with the approved software. No removable media may be brought in from an external source e.g. the employee's home, and used on the company's system at any time.
- Subject to the above paragraph, employees must not download unauthorised software or electronic files without implementing virus protection. All files attached to external email as well as files downloaded from the internet must be scanned. Users must report suspected incidents of software viruses or similar contaminants from email attachments and/or downloads from the internet immediately to a member of staff responsible for IT systems.
- Extreme care must be taken when sharing passwords, encryption keys and other confidential information relating to the company's systems. Any sharing of such information must be done so using secure encryption methods. If feasible, passwords to files should be shared verbally once the correct identify of the person has been established.
- Employees must not change or use another person's files, output or username for which they do not have express authorisation. Employees should lock or switch off their computer when away from it.

8. Monitoring

The company may deny access to the internet and its electronic mail services, and may inspect, monitor, log, track or disclose email or internet access activities in, but not limited to, the following circumstances.

- If there are substantiated reasons to believe that violations of the law and/or this policy have taken place which provide the company with good cause or
- A bona fide complaint is received in relation to misuse of email or internet access.
- By accessing the internet and electronic mail services through facilities provided by the company the user acknowledges that the company can monitor and examine at any time all individual connections and communications. The company respects the privacy of internet and email users and will not routinely inspect, monitor, log, track or disclose email or internet access activities without having good cause.

9. Contracts

Employees should be aware that contracts that can bind the company can be created on the internet or by email. Employees must not enter into contracts or subscribe for, order, purchase, sell or advertise for sale any goods or services on the internet or by email, unless with the express authorisation of the company.

10. Confidentiality

- Email can be inadvertently sent to the wrong address. It may also be read by someone other than the intended recipient. Caution must be exercised at all times when communicating proprietary, confidentially sensitive information or information relating to the company when using email systems and users should ensure that such information is properly encrypted and that they have the authority to send it.
- No client or customer related information should be sent over any public computer system without the prior written consent of the client or customer.
- All documentation and intellectual property remain the property of 'The Company'.

11. Copy Right

Employees must adhere to all intellectual property and copyright law. Employees must not upload, download or otherwise transmit any copyrighted materials belonging to parties outside the company without the copyright holder's written permission.

12. Personal Use

Company email and internet systems may not be used for personal purposes during normal working hours. Occasional use for personal reasons is allowed outside working hours subject to the terms and conditions of this policy. The use of web-based email systems such as "hotmail" and "yahoo" may be used by full time members of staff only and at the continuing

discerns of 'The Board' thus avoiding company email accounts being used inappropriately. The company reserves the right to block access to personal emails systems and other sites at its discretion.

Personal external email sent via a company access account should clearly indicate that it is a personal communication and not related to and does not express the views of the company. Users are expected to respect and not abuse the privilege of personal email and specifically must not.

1. Use company email systems, content and mailing list for personal gain.
2. Directly or indirectly interfere with the operation of email services, and cause unwarranted or unsolicited interference with the use of email systems by others.
3. Interfere with employment duties, or other obligations to the company; or burden the company with noticeable system congestion and/or additional costs. Any sources causing such congestion and/or additional costs will be blocked automatically and will not be permitted access to our mail system.
4. Hold personal files e.g. pictures on 'The Company's' servers

The records arising from personal use of email will be treated no differently from other email when applying this policy in respect of confidentiality, privacy, disclosure and technical administration.

13. Company Telephones

The company's telephones are intended for business use only, prior permission must be sought before making personal calls, which should only be of an urgent/essential nature. Abuse of this rule will not be tolerated.

Similarly, employees should advise their families and friends that incoming calls must be restricted to urgent/essential matters only.

Employees who choose to ignore these rules will be liable to the company for the cost of personal calls, they may also become liable for disciplinary action.

14. Disciplinary

Any breach of this policy may be subject to disciplinary action, up to and including dismissal and may result in criminal prosecution.

These policies supplement your terms of employment but are not of contractual effect. Their purpose is to explain the Company's current policies and procedures but they may be subject to change without notice if changes are considered appropriate by the Company or if there are changes in relevant legislation.