Communications, Email and Internet Policy

Introduction

1.1 This Communications, Email and Internet Policy applies to all employees, contractors and agents of Health and Safety Partnership Consultants Limited ("the Company") who use the communications equipment and systems provided by the Company ("Users").

1.2 Users are encouraged to use email and the internet at work as a fast and reliable method of communication with significant advantages for business.

1.3 In light of the fact that communications made by Users reflect upon the Company and are capable of creating a number of commercial, professional and legal problems, this policy is intended to clarify what the Company expects from Users and their responsibilities when using the Company's communications facilities.

1.4 "Communications facilities", "communications equipment" and "communications systems" include:

1.4.1 Telephone;

1.4.2 Fax;

1.4.3 Email;

1.4.4 Internet and Intranet;

1.4.5 Video conferencing facilities, including Skype, Zoom, MS Teams etc.

And any other communication device or network provided by the Company.

1.5 Whilst the communications equipment and systems provided by the Company are made available to Users for the purposes of the business, a certain amount of limited personal use is permitted insofar as such personal use is consistent with this Communications Policy and the duties of the User.

General Principles

There are certain general principles that should be borne in mind when using any type of communication, be it external or internal, including hard copy letters, memos and notices. The Company expects all Users to:

1.6 Use communications equipment and facilities, including Company letterheads and stationery, responsibly and professionally and at all times in accordance with their duties;

1.7 Be mindful of what constitutes confidential or restricted information and ensure that such information is never disseminated in the course of communications without express authority;

1.8 Ensure that they do not breach any copyright or other intellectual property right when making communications;

1.9 Ensure that they do not bind themselves or the Company to any agreement without express authority to do so;

1.10 Be aware of email trails when forwarding emails, and if necessary delete email content below their messages;

1.11 Be mindful of the fact that any communication may be required to be relied upon in court, to the advantage or the detriment of the individual or the Company and conduct their use of communication systems and equipment accordingly.

Internet

1.12 The Company provides access to the internet for the sole purpose of business and to assist Users in the furtherance of their duties. However, the Company recognises that Users may need to use the internet for personal purposes and such use is permitted provided it is reasonable and does not interfere with the User's performance of his/her duties. Users may be asked to justify the amount of time they have

spent on the internet or the sites they have visited.

1.13 Users must not use the internet to gain or attempt to gain unauthorised access to computer material or private databases, including restricted areas of the Company's network. Nor must they intentionally or recklessly introduce any form of malware, spyware, virus or other malicious software or code to the communications equipment or systems of the Company.

1.14 Users must not access or attempt to access any information which they know or ought to know is confidential or restricted.

1.15 User are not allowed to access the Dark Web **for any reason**, on company equipment;

1.16 Users must not download or install any software without the express permission of the Managing Director.

1.17 Users must not attempt to download, view or otherwise retrieve illegal, pornographic, sexist, racist, offensive or any other material which may cause embarrassment to the corporate image of the Company. Any such attempt will constitute a disciplinary offence and in addition to internet access being reviewed, reduced or withdrawn, may be subject to disciplinary action or summary dismissal.

Blogging and Social Networking Sites

1.18 The viewing of or contribution to blogs, content sharing and social networking sites such as "Facebook", "Myspace", "Bebo", "Instagram", "OnlyFans" and "YouTube" using the Company's communications systems is prohibited.

1.19 Authorised employees are allowed to contribute to the **Company** LinkedIn and Twitter account but must not express personal opinion, they may only post Company approved content;

1.20 The Company recognises that in their private time Users may wish to publish content on the internet through a variety of means. Even outside of work Users must adhere to this policy when creating, modifying or contributing to websites.

1.21 If a User makes any posting, contribution or creation or publishes any other content which identifies or could identify the User as an employee, contractor, agent or other member or associate of the Company, or in which the User discusses his/her work or experiences relating to the Company, the User must at all times ensure that his/her conduct is appropriate and consistent with their contract of employment and the corporate image of the Company, and should bear in mind that the User as an employee owes a duty of fidelity to the Company.

1.22 If a User is unsure as to the appropriateness of a posting or other content published by him/her, they should speak to the Managing Director at the earliest opportunity to seek clarification and before posting.

1.23 If, in any contribution or posting which identifies or could identify the User as an employee, agent or other affiliate of the Company, the User expresses an idea or opinion he/she should include a disclaimer which clearly states that the opinion or idea expressed is that of the User and does not represent that of the Company.

Email

Company Email

1.24 The Company recognises that there may be instances where Users may need to use their Company email address for personal reasons. This is permitted on the condition that such use is kept to a minimum and does not interfere with the performance of the User's duties. In any case Users are not permitted to use their Company email address to subscribe to any newsletters or to receive any marketing, as this will result in extra unnecessary burden being placed upon the Company's communications systems.

1.25 If Users do use the Company email for personal reasons, they will be deemed to agree to the possibility that any emails sent or received may be subject to monitoring in accordance with this policy.

1.26 Users should at all times remember that email messages may have to be disclosed as evidence for any

court proceedings or investigations by regulatory bodies and may therefore be prejudicial to both their and the Company's interests. Users should remember that data which appears to have been deleted is often recoverable.

Personal Email

1.27 Users are permitted to access and use their personal email accounts only to the extent that such use is reasonable and in accordance with this policy.

Telephone Use

Company Telephone System

1.28 The Company's telephone lines are for the exclusive use by Users working on the Company's business. Essential personal telephone calls regarding Users' domestic arrangements are acceptable, but excessive use of the Company's telephone system for personal calls is prohibited. Acceptable telephone use may be defined as no more than twenty minutes of personal calls in a working day. Any personal telephone calls should be timed to cause minimal disruption to Users' work.

1.29 Users should be aware that telephone calls made and received on the Company's telephone system may be routinely monitored to ensure customer satisfaction or to check the telephone system is not being abused.

1.30 If the Company discovers that the telephone system has been used excessively for personal calls, this will be dealt with under the Company's disciplinary procedures.

Mobile Phones

1.31 Essential personal telephone calls regarding Users' domestic arrangements are acceptable but excessive use of Users' own mobile phones for personal calls (also texting, emailing, chat apps such as WhatsApp, Snapchat, Messenger services (including Facebook Messenger) and web browsing) is prohibited. In order to avoid disruption to others, mobile phones should be set to silent during normal working hours.

1.32 Any personal telephone calls on Users' own mobile phones should be timed to cause minimal disruption to Users' work and to colleagues working nearby.

Security

1.33 The integrity of the Company's business relies on the security of its communications equipment and systems. Users bear the responsibility of preserving the security of communications equipment and systems through careful and cautious use.

1.34 Access to certain websites is blocked from Company communications equipment and systems. Often the decision to block a website is based on potential security risks that the site poses. Users must not attempt to circumvent any blocks placed on any website or features by the Company.

1.35 The Company provided VPN (Norton) must be active on all communication devices at all times.

1.36 Users must not download or install any software or program without the express permission of the Managing Director.

1.37 Users must not share any password that they use for accessing Company communications equipment and systems with any person, other than when it is necessary for maintenance or repairs by HSPCL IT staff. Where it has been necessary to share a password, the User should change the password immediately when it is no longer required by HSPCL IT Staff Users are reminded that it is good practice to change passwords regularly.

1.38 Users must ensure that confidential and sensitive information is kept secure. Workstations and screens should be locked when the User is away from the machine, hard copy files and documents should be secured when not in use and caution should be exercised when using mobile telephones outside of the workplace.

1.39 When opening email from external sources Users must exercise caution in light of the risk viruses pose to system security. Users should always ensure that they know what an attachment is before opening it.

If a User suspects that their computer has been affected by a virus they must contact Managing Director immediately.

1.40 No external equipment or device may be connected to or used in conjunction with the Company's equipment or systems without the prior express permission of Managing Director.

Monitoring

1.41 The Company may monitor Users' communications for the following reasons:

1.41.1 To ensure Company policies and guidelines are followed, and standards of service are maintained;

1.41.2 To provide evidence of transactions and communications;

1.41.3 To help combat unauthorised use of the Company's communications equipment and systems and maintain security;

1.41.4 If the Company suspects that a User has been viewing or sending offensive or illegal material;

1.41.5 If the Company suspects that a User has been spending an excessive amount of time viewing non work-related sites and/or sending and receiving an excessive number of personal emails;

1.41.6 In order to better understand the requirements of the Company in terms of the provision of communications equipment and systems.

1.42 Users should be aware that all internet and email traffic data sent and received using the Company's communication systems is logged, including websites visited, times of visits and duration of visits. Any personal use of the internet will necessarily therefore be logged also. Users who wish to avoid the possibility of the Company becoming aware of any political or religious beliefs or affiliations should avoid visiting websites at work which might reveal such affiliations. By using the Company's communications equipment and systems for personal use, Users are taken to consent to personal communications being logged and monitored by the Company. The Company shall ensure that any monitoring of communications complies with the General Data Protection Regulations.

1.43 Private browser **must not** be enabled on any company equipment.

1.44 When monitoring emails, the Company will normally restrict itself to looking at the address and heading of the emails. However, if it is considered necessary, the Company may open and read emails. Users should be aware that sensitive and confidential communications should not be sent by email because it cannot be guaranteed to be private.

Misuse and Compliance

1.45 Any User found to be misusing the communications equipment and systems provided by the Company will be treated in line with the usual disciplinary procedure.

1.46 The viewing, transmission, downloading, uploading or accessing in any way of any of the following material using Company communications equipment and systems will amount to gross misconduct with the possibility of summary dismissal:

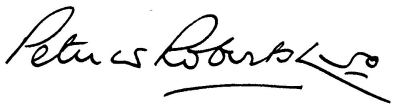
1.46.1 Material which is pornographic, sexist, racist, homophobic, paedophilic or any other discriminatory or otherwise offensive material;

1.46.2 Illegal or criminal material, including material which breaches copyright or any other intellectual property right;

1.46.3 Any material which has the object or effect of causing harassment to the recipient;

1.46.4 Material which the User knows, or ought to know, is confidential or restricted information and which they are not authorised to deal with.

Signed:



Position: **Director**

Latest review dated: **01 January 2023**