

Email Processing Communications Policy

Approved by: Dave Pattinson Managing Director

Issue Date: 19th September 2023
Last Review Date: 9th August 2024
Next Review Date: 9th August 2025
Ref: PV 25

Print Date: 12 August 2024 at 9:32 AM

This policy will be reviewed annually or earlier if significant changes occur, to ensure its continuing suitability, adequacy, and effectiveness.

Email and Electronic Communication, Internet Policy

VIRUS PROTECTION PROCEDURES

In order to prevent the introduction of virus contamination into the software system the following procedure must be observed:

- a) The procedure for unauthorised software including public domain software, USBs, external hard drives, CDs or internet downloads must not be used; and is monitored by managers and (social link up) daily.
- b) all software must be virus checked using standard testing procedures before being used. This will involve the management testing external devices, using (eset) anti virus which is installed on all IT equipment, and the package is set to inspect all devices automatically.

USE OF COMPUTER EQUIPMENT

In order to control the use of the Company's computer equipment and reduce the risk of contamination the following will apply:

- a) the introduction of new software must first of all be checked and authorised by David Pattinson before general use will be permitted;
- b) only authorised staff have access to the Company's computer equipment;
- c) only authorised software may be used on any of the Company's or clients computer equipment;
- d) only software that is used for business applications may be used;
- e) no software may be brought onto or taken from the Company's premises without prior authorisation by Dave Pattinson;
- f) unauthorised access to the computer facility or clients computers will result in disciplinary action; and investigated fully, by an appointed manager.
- g) unauthorised copying and/or removal of computer equipment/software will result in disciplinary action, such actions could lead to dismissal.

E-MAIL AND INTERNET POLICY

1) Introduction

The purpose of the Internet and E-mail policy is to provide a framework to ensure that there is continuity of procedures in the usage of internet and e-mail within the Company. The internet and e-mail system have established themselves as an important communications facility within the Company and have provided us with contact with professional and academic sources throughout the world. Therefore, to ensure that we are able to utilise the system to its optimum we have devised a policy that provides maximum use of the facility whilst ensuring compliance with the legislation throughout.

2) Internet

Where appropriate, duly authorised staff are encouraged to make use of the Internet as part of their official and professional activities. Attention must be paid to ensuring that published information has relevance to normal professional activities before material is released in the Company or clients name. Where personal views are expressed a disclaimer stating that this is the case should be clearly added to all correspondence. The intellectual property right

and copyright must not be compromised when publishing on the Internet. The availability and variety of information on the Internet has meant that it can be used to obtain material reasonably considered to be offensive.

The use of the Internet to access and/or distribute any kind of offensive material, or material that is not work-related, leaves an individual liable to disciplinary action which could lead to dismissal.

3) Procedures – Acceptable/Unacceptable Use

- a) unauthorised or inappropriate use of the internet system may result in disciplinary action which could result in summary dismissal.
- b) the internet system is available for legitimate business use and matters concerned directly with the job being done. Employees using the internet system should give particular attention to the following points:
 - i) comply with all of our internet standards;
 - ii) access during working hours should be for business use only;
 - iii) private use of the internet should be used outside of your normal working hours.
- c) the Company will not tolerate the use of the Internet system for unofficial or inappropriate purposes, including:
 - i) accessing websites which put our internet at risk of (including but not limited to) viruses, compromising our copyright or intellectual property rights;
 - ii) non-compliance of our social networking policy;
 - iii) connecting, posting or downloading any information unrelated to their employment and in particular pornographic or other offensive material;
 - iv) engaging in computer hacking and other related activities, or attempting to disable or compromise security of information contained on the Company's or clients computers.

You are reminded that such activities (iii. and iv.) may constitute a criminal offence.

4) E-mail

The use of the e-mail system is encouraged as its appropriate use facilitates efficiency. Used correctly it is a facility that is of assistance to employees. Inappropriate use however causes many problems including distractions, time wasting and legal claims. The procedure sets out the Company's position on the correct use of the e-mail system. If a manager or appointed person with access to works emails, or other communication methods electronically, is incapacitated, on leave sickness, out of office or other. All staff are reminded, then its checked by senior management, that staff have diverted all communications directly or indirectly to the second or third in command, Stacey Vivian and Alan Snelson or Dave Pattinson, in the event of communications come through to the company, and information, requests or actions are required. A nominated person or persons can pick up the communications and follow then up, and action if necessary. Then on the return of the said person, they can be informed that actions have been taken in their absence, and all follow ups for this policy is being carried out. Dave Pattinson will request (social linkup) to divert all communications to him, and he will also ask managers to cc him in all communications.

5) Procedures - Authorised Use

- a) unauthorised or inappropriate use of the e-mail system may result in disciplinary action which could include summary dismissal, after investigation this is found to be correct. A manager will check this daily by checking the history logs, and asking our service host provider (social Linkup) to check history use also.

b) the e-mail system is available for communication and matters directly concerned with the legitimate business of the Company. Employees using the e-mail system should give particular attention to the following points:

- i) all comply with Company communication standards;
- ii) e-mail messages and copies should only be sent to those for whom they are particularly relevant;
- iii) e-mail should not be used as a substitute for face-to-face communication or telephone contact, these methods should be used as a first option. Abusive e-mails must not be sent. Hasty messages sent without proper consideration can cause upset, concern or misunderstanding; this is the responsibility of the user to manage, and all emails are also monitored by a manager and also (social linkup).
- iv) if the e-mail is confidential the user must ensure that the necessary steps are taken to protect confidentiality. The Company will be liable for infringing copyright or any defamatory information that is circulated either within the Company or to external users of the system; and
- v) offers or contracts transmitted by e-mail are as legally binding on the Company as those sent on paper.

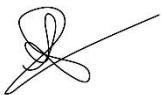
c) The Company will not tolerate the use of the e-mail system for unofficial or inappropriate purposes, including:

- i) any messages that could constitute bullying, harassment or other detriment;
- ii) personal use (e.g. social invitations, personal messages, jokes, cartoons, chain letters or other private matters); this is monitored by a manager and also (social linkup).
- iii) on-line gambling;
- iv) accessing or transmitting pornography;
- v) transmitting copyright information and/or any software available to the user; or
- vi) posting confidential information about other employees, the Company or its clients or suppliers.

6) Monitoring

We reserve the right to monitor all e-mail/internet activity by you for the purposes of ensuring compliance with our policies and procedures and of ensuring compliance with the relevant regulatory requirements. This includes monitoring of any additional accounts you may be requested to set up for the purposes of performing your work tasks, which are subject to the same rules as your work email account. Information acquired through such monitoring may be used as evidence in disciplinary proceedings. Monitoring your usage will mean processing your personal data. You may read more about the data we hold on you, why we hold it and the lawful basis that applies in the employee privacy notice.

Approved by: Dave Pattinson Managing Director



Issue Date: 19th September 2023
Last Review Date: 9th August 2024
Next Review Date 9th August 2025

Ref: PV 25

Print Date: 12 August 2024 at 9:32 AM