TELEPHONE, MOBILE & INTERNET POLICY

TELEPHONE, MOBILE & INTERNET POLICY

Zeal ("the company") provides this policy to set out guidance relating to telephone, mobile and internet use by employees. Inappropriate use of mobile, telephone and internet at work decreases productivity, causes security risks, distracts co-workers and colleagues, and can cause significant expense to a business. This policy is designed to set down minimum standards regarding mobile phone, telephone and internet use for all employees during their employment with the Company. In so far as this policy imposes any obligations on the Company, those obligations are not contractual and do not give rise to any contractual rights. To the extent that this policy describes benefits and entitlements for employees, they are discretionary in nature and are also not intended to be contractual. The terms and conditions of employment that are intended to be contractual are set out in an employee's written employment contract. The Company may unilaterally introduce, vary, remove or replace this policy at any time.

TELEPHONE & MOBILE PHONE USE

The Company appreciates that staff may have a need to make and receive some personal telephone calls during work hours. However, unless in the case of an emergency, telephone and mobile phone use should never interfere with employees' work duties, including but not limited to the service of customers.

The following guidelines govern the use of telephones and mobile phones and the making and/or receiving of personal calls during work time:

- Personal calls should never take precedence over the service of customers and clients. Unless there is an emergency, all personal phone calls should be restricted to legitimate work breaks (for example, your meal break) or before or after the commencement of your shift;
- Any workplace telephones are provided for the conduct of the Company's business. Such telephones should not be used for

personal calls except in the case of emergency, or where you have permission to make or receive personal calls by your manager. Any use of Company telephones for the conduct of any other business or for the financial gain of any other party is expressly prohibited;

- All personal calls during the performance of your work duties, should be kept as short as possible in the interests of minimising disruption to work;
- Employees must not use Company telephones (including mobile phones) in any way that offends the law or as a device for delivery of offensive or objectionable communications. Offences of this nature may result in disciplinary action up to an including termination of employment;
- Where you are provided with a Company mobile phone it is provided solely for performance of your work duties, unless the Company informs you otherwise. The Company will only pay for legitimate work calls and you may be required to pay for personal phone usage (unless you are informed otherwise). The Company acknowledges that employees may need to access and use the internet to carry out their duties and to send and receive emails. In order to provide employees with clear expectations as to what is and what is not an appropriate use of the internet and email at work, the following guidelines have been developed.

This policy applies to the use of the Company's internet and email services whilst employees are at work, and when employees access such services outside of work hours (for example when they take a Company laptop home or on a business trip or client visit).

This policy also applies to the use of personal equipment (eg mobile phones and personal computers) that are used to access Company systems or emails.

Please remember that your work emails are property of the Company, as are all programs and files used on the Company's internet and computer systems. You should therefore use all such systems and materials appropriately in accordance with your work duties and follow any directions given to you by the Company regarding their use.

On request you must provide all password and login details used in connection with your work duties to the Company. You must also return all Company equipment and materials (eg laptops, USB drives, Company data saved in other locations, etc) on request and upon termination of your employment.

As far as is reasonably possible, the Company will respect the privacy of individuals in the application and enforcement of this policy.

- Only use the internet and email for legitimate business purposes related to your job;
- Permission from your manager may be sought to use the Company internet in non-work time for study, research or other reasonable purpose;
- Do not use the Company internet or email for personal use. In particular, you should not access personal emails, or social media unless specific permission of your manager has been obtained;
- Do not use the Company internet or email for personal gain or the benefits of persons other than the Company;
- Do not use the Company internet or email to send defamatory, threatening, sexually explicit, offensive or obscene messages or images to other employees or to anyone outside the Company;
- Do not use the Company internet or email to send messages or images that are discriminatory (such as those which are racist or involve sexual harassment) to other employees or to anyone outside the Company;
- Do not use the Company internet or email in any way which involves sending or accessing material that is unlawful or illegal;
- Do not use the Company internet or email to download, upload, retrieve or send a sexually explicit, racist or otherwise discriminatory, illegal or unlawful, offensive or obscene material while you are on work premises (even if using your personal equipment), or while using Company computers or systems inside or outside of work premises;

- Do not access without permission (hack) any computer, whether owned by the Company or by any other organisation;
- When you send emails or use the Company internet, do not disclose confidential information, unless this is necessary for the performance of your work duties; permission;
- Do not use the Company internet or email for the creation of legal or contractual obligations that bind the Company unless specifically authorised to do so by your manager;
- Do not use the Company's systems, internet or wi-fi to connect to personal services (such as personal email services) during working hours using Company or personal equipment;
- Do not use another employee's computer or email to carry out any of the activities prohibited above

SECURITY

Employees must ensure that the Company's confidential information, intellectual property and hardware is secured at all times whether in the workplace, when working remotely or in transit.

Employees should:

- Ensure all devices are password protected and locked when not in use;
- Only connect devices to WiFi at secure locations such as your home or workplace. Do not connect to unsecured WiFi networks in public places;
- Promptly report the loss of theft of any devices with access to the Company's proprietary information or systems;
- Not download or open any suspicious emails or files without first checking with a manager or IT department;

- Virus scan any material before uploading it into the Company's network or PC's;
- Obtain permission before downloading any material onto a USB or cloud.

BREACH OF THIS POLICY

A breach of this policy may result in disciplinary action up to and including termination of employment. In addition, unlawful or illegal use of the Company's internet or email systems may constitute a civil or criminal offence for which you could be personally liable.

OTHER POLICIES

Employees are encouraged to read this policy in conjunction with other relevant Company policies, including:

- Code of Conduct