INFORMATION TECHNOLOGY AND COMMUNICATIONS POLICY

To maximise the benefits of our computer and communication resources and minimise potential liability, you are only permitted to use our various communication systems in accordance with the following guidelines.

Technology and the law change regularly, and this policy will be updated to take account of these changes as and when necessary. You will be informed when the policy has changed but it is your responsibility to read the latest version of this document.

General Rules

Our computers, telephone and communication systems, software and their contents are intended for business purposes. You are permitted to use the systems to assist you in performing your job.

We have the right to monitor and access all aspects of our systems, including data, which is stored on our computer systems, in compliance with the Data Protection Act 1998.

You must receive prior approval from management before using any part of our computer systems for personal use.

Security

We require you to log on to our computer systems using your own password (where provided) which must be kept secret. You should select a password that is not easily broken (e.g., not your surname).

You are not permitted to use another employee's password to log on to our computer system, whether or not you have permission to do so. If you log on to the computer, deliberately using another employee's password, you will be liable to disciplinary action up to and including summary dismissal on the grounds of gross misconduct.

If you deliberately disclose your password to another employee, you will be liable to similar disciplinary action up to and including summary dismissal on the grounds of gross misconduct.

To safeguard our computer systems from viruses, you are not permitted to load or run unauthorised games or software, or to open documents or communications from unknown origins.

We reserve the right to require you to hand over all data relevant to our business held in computer useable format.

USE OF E-MAIL

We encourage you to use e-mail and the internet at work where this can save time and expense. However, we require you to follow our strict rules below.

If you are unsure about whether something you propose to download or to which you intend to respond may breach this policy you should seek advice from your Line Manager immediately.

Although we encourage the use of e-mail and the internet where appropriate, their use entails some risks. Accordingly, you must be prudent and take care not to introduce viruses onto our system and you must take proper account of any security advice we give to you.

You should also ensure that you do not send libellous statements in e-mails or use e-mail in an unprofessional way; such actions could expose us to the risk of legal action and liability for damages.

These rules are designed to minimise the legal risks to the business when you use e-mail at work and access the internet. Where something is not specifically covered in this policy, you should seek advice from your Line Manager.

Contents

E-mails should be checked very carefully prior to sending. E-mail should be treated like any other form of written communication and, as such, what is normally regarded as unacceptable in a letter is equally unacceptable in an e-mail communication. The content of any e-mail sent by you should be in accordance with the principles set out in our Equal Opportunity Policy and our Dignity at Work Policy.

The use of e-mail to send or forward messages which are defamatory, obscene or otherwise inappropriate will be treated as misconduct under our Discipline and Dismissal Procedure. In serious cases this could be regarded as gross misconduct and lead to your dismissal.

Other examples of misuse include, but are not limited to, the following:

- sending, receiving, downloading, displaying, or disseminating material that insults, causes offence, or harasses others.
- accessing pornographic, racist, or other inappropriate or unlawful materials.
- engaging in online chat rooms or gambling.
- forwarding electronic chain letters or similar material.
- downloading or disseminating copyright materials.
- transmitting confidential information about us or our clients.
- downloading or playing computer games; and
- copying or downloading software

Equally, if you receive an obscene or defamatory e-mail, whether unwittingly or otherwise, and from whatever source, you should not forward it to any other address.

Statements to avoid in e-mails include those criticising our competitors or their staff, those stating that there are quality problems with goods or services of suppliers or customers and clients, and those stating that anyone with whom we have dealings is incompetent.

PALMTOP/HAND-HELD COMPUTERS

Lap-top computers e.g., iPads issued to you always remain our property and may be withdrawn if there is any evidence that they have been misused.

Appropriate use

Where appropriate to your role we may provide you with a palmtop/hand-held computer for work-related purposes, i.e., to enable you to communicate effectively on matters relating to our organisation. They should not be used for personal purposes.

You may not at any time use the palmtop/hand-held computers issued to:

- communicate information that is confidential to the organisation, unless authorised to do so.
- send or forward any message (inside or outside the organisation) that could constitute bullying or harassment or be interpreted as offensive; or
- send personal messages, jokes, cartoons, or chain letters to any person inside or outside of the organisation.

Although you are expected to use your palmtop/hand-held computers for the purpose of performing your role efficiently, this does not mean that you are expected to be "on-call" at all times. You have the right to maintain a reasonable work-life balance.

Etiquette

Although it is recognised that a laptop/hand-held computers issued to you is, like a mobile phone, an indispensable tool, you should endeavour not to overuse it or to use it inappropriately.

When attending a business meeting or training course, you should ensure your palmtop/hand-held computers is switched off.

The style and content of messages created using your palmtop/hand-held computer should be in line with our policy covering e-mail messages. You should prepare your communications with care, and they should be professional in their tone.

Safety/security

If you are issued with a palmtop/hand-held computer, you must take proper care of it and always ensure its security. For example, palmtop/hand-held computers should not be left unattended in parked cars.

If, as a result of your carelessness or negligence, your laptop/handheld computer is lost or damaged, we reserve the right to take appropriate disciplinary action against you and deduct the cost of replacement or repair from your salary or wage.

Monitoring

We carry out monitoring of our computer equipment, including palmtop/hand-held computers, for security reasons to detect and deter unauthorised use.

Monitoring will consist of random checks on your computer equipment. The results of the monitoring will be maintained in strict confidence.

Mobile telephones

Our mobile telephones are provided at our absolute discretion based on business need.

We monitor the use of our mobile telephones.

It is your responsibility to safeguard any mobile telephone provided to you. Please do not leave a mobile phone in a visible place such as in an unattended car. The use of a personal identification number (PIN) is recommended for added security. Loss of one of our mobile telephones should be reported to your Line Manager.

Etiquette

You should always display due consideration for others in the use of your mobile telephone; this entails turning it off or putting it on silent when your use of it could be distracting, for example during meetings and training sessions.

You should also observe any restrictions imposed by other organisations on the use of mobile telephones while you are on their premises or on premises under their control.

SOCIAL NETWORKING

We do not permit you to access social networking websites using our IT system while at work. If you access social networking sites using your own palmtop computer while at work, you must do so only during authorised breaks.

Personal conduct

We respect your right to a private life. However, we must also ensure that confidentiality and our reputation are protected. Accordingly, while using social networking websites at any time, we require you to:

- ensure that you do not conduct yourself in a way that is detrimental to us;
- take care not to allow your interaction on these websites to damage working relationships between members of staff and our clients; and

- if you have social networking 'friends' who are clients please take additional care to ensure you do not conduct yourself in a way that may damage the reputation of the firm or harm our commercial relationships.

Failure to do so may result in disciplinary action, up to and including summary dismissal, being taken against you.

You should note if you have a Facebook page/twitter account or other social network platform you will be regarded by us as responsible for any comments, tweets or posts found on your page regardless of whether made by you personally or not.

Security and identity theft

You should be aware that social networking websites are a public forum, particularly if you are part of a "network". You should not assume that your entries on any website will remain private. You should never send abusive or defamatory messages.

You must also be security conscious and should take steps to protect yourself from identity theft by restricting the amount of personal information that you give out.

Social networking websites allow people to post detailed personal information such as date of birth, place of birth and favourite football team, which can form the basis of security questions and passwords. In addition, you should:

- ensure that no information is made available that could provide a person with unauthorised access to our business and/or any confidential information; and
- refrain from recording any confidential information about us on any social networking website.

Breach of this policy

Any breach of this policy will be treated as misconduct. Whether it is minor or gross misconduct will depend on the circumstances.

Queries

If you have any questions about this policy, you should refer them to your Line Manager.

This policy statement will be regularly reviewed and updated, as necessary. The management team endorses these policy statements and are fully committed to their implementation.

Signed_____Date: 31/05/2021

G. Kennedy, Managing Director

Campbell & Kennedy Maintenance Attitude is everything	INFORMATION TECHNOLOGY AND COMMUNICATIONS POLICY	IMPL-39	
		Revision:	2.0
		Date:	31/05/2021
		Approved by	GK

Unit A19 Whitecrook Business Centre
78 Whitecrook Street
Clydebank, G81 1QF
T 0141 952 1933
E operationsl@ckmaintenence.co.uk

W www.campbellkennedy.co.uk

Registered in Scotland SC273475

CK Technology