METAC Policy & Procedure for Communications and GDPR

Issue No.	Date	Approved by:	Details of Change
1			

A) INTRODUCTION

1) IT and Communication plays an essential role in the conduct of our business. The IT infrastructure including e-mail and internet access have therefore significantly improved business operations and efficiencies.

2) How you communicate with people not only reflects on you as an individual but also on METAC as a business. As a result of this METAC values your ability to communicate with colleagues, clients/customers, and business contacts but we must also ensure that such systems and access are managed correctly, not abused in how there are used or what they are used for,

3) This policy applies to all members of METAC who use our or our clients' communications facilities, whether Directors/Consultants, full or part-time employees, contract staff or temporary staff. The parameters and restrictions are outlined below, and you are required to read them carefully.

B) GENERAL PRINCIPLES

1) You must use our and our clients' information technology and communications facilities sensibly, professionally, lawfully, consistently with your duties and in accordance with this policy and other Company rules and procedures.

2) At all times employees must behave with honesty and integrity and respect the rights and privacy of others in relation to electronic communication and information. The company reserves the right to maintain all electronic communication and files.

3) Every employee will be given access to the Intranet and/or Internet as appropriate to their job needs.

4) All PC/network access will be through passwords, and no individual is permitted onto the system using another employee's password. Employees are not permitted to share their password with anyone inside or outside the company.

5) All information relating to our clients/customers and our business operations is confidential. You must treat our paper-based and electronic information with utmost care.

6) Many aspects of communication are protected by intellectual property rights which can be infringed in several ways. Downloading, copying, possessing and distributing material from the internet may be an infringement of copyright or of other intellectual property rights.

7) Care must be taken when using e-mail as a means of communication because all expressions of fact, intention and opinion in an e-mail may bind you and/or the Company and can be produced in court in the same way as other kinds of written statements.

8) If you are speaking with someone face to face, via the telephone, in writing via whatever medium you are a representative of the Company. Whilst in this role you should not express any personal opinion that you know, or suspect might be contrary to the opinions of the Directors or Company policy.

9) You must not use any of our or our clients' media to do or say anything which would be subject to disciplinary or legal action in any other context such as sending any sexist, racist, defamatory or other unlawful material. If you are in doubt about a course of action, take advice from a member of management.

C) USE OF ELECTRONIC MAIL

1) **Business use**

Always use the "Bcc" box when mailing to groups whenever the members of the group are unaware of the identity of all the others (as in the case of marketing mailing lists), or where you judge that the membership of the group of one or more individuals should perhaps not be disclosed to the others, because if you use the "cc" box each recipient is informed of the identity (and in the case of external recipients, the address) of all the others. Such a disclosure may breach any duty of confidence owed to each recipient, breach the Company's obligations under the General Data Protection Regulation and Data Protection Acts or may inadvertently disclose confidential business information such as a marketing list. This applies to both external and internal e-mail.

Expressly agree with the customer/client that the use of e-mail is an acceptable form of communication bearing in mind that if the material is confidential, privileged or commercially sensitive then un-encrypted e-mail is not secure.

If you have sent an important document, always telephone to confirm that the e-mail has been received and read.

Considering the security risks inherent in web-based e-mail accounts, you must not e-mail business documents to your personal web-based accounts. You may send documents to a customer's/client's web-based account if you have the customer's/client's express written permission to do so. However, under no circumstances should you send sensitive or highly confidential documents to a customer's/client's personal web-based e-mail account (e.g. Yahoo, or Hotmail), even if the customer/client asks you to do so.

The following two messages must be included on all e-mails sent from your e-mail and be located under your Signature and Company Logo:

1. CONFIDENTIALITY NOTICE:

This e-mail message and accompanying data are for the sole use of the intended recipient (s) and may contain information that is confidential. If you are not the intended recipient, you are notified that any use, dissemination, distribution or copying of this message or data is prohibited. If you have received this message in error, please notify us immediately and erase all copies of the message and attachments. Thank you.

2. Please note that cyber-crime is a real danger. If you are transferring funds by way of electronic bank transfer to METAC Training you must verify the companies bank account details, by prior telephone call with the METAC Representative you are dealing with or the companies accounts department. METAC Training does not accept responsibility or liability in the event that any party suffers loss as a result of cyber-crime. We will never contact you by email regarding changes to our bank account details. Thank you.

2) **Personal use**

a) Although our e-mail facilities are provided for the purposes of our business, we accept that you may occasionally want to use them for your own personal purposes. This is permitted on condition that all the procedures and rules set out in this policy are complied with. Be aware, however, that if you choose to make use of our facilities for personal correspondence, the Company may need to monitor communications for the reasons shown below.

b) Under no circumstances may the Company's facilities be used in connection with the operation or management of any business other than that of the Company or a customer/client of the Company unless express permission has been obtained from a member of management.

c) You must ensure that your personal e-mail use:

- does not interfere with the performance of your duties.
- does not take priority over your work responsibilities.
- does not cause unwarranted expense or liability to be incurred by the Company or our clients.
- does not have a negative impact on our business in any way; and
- is lawful and complies with this policy.

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

- any messages that could constitute bullying, harassment or other detriment.
- on-line gambling.
- accessing or transmitting pornography.
- transmitting copyright information and/or any software available to the user; or
- posting confidential information about other employees, the Company or its customers or suppliers.

D) USE OF INTERNET AND INTRANET

1) We trust you to use the internet sensibly. Although internet facilities are provided for the purposes of our business, we accept that you may occasionally want to use them for your own personal purposes. This is permitted on condition that all the procedures and rules set out in this policy are complied with and your use of the internet does not interfere in any way with the performance of your duties.

2) Whenever you access a web site, you should always comply with the terms and conditions governing its use. Care must be taken in the use of information accessed through the Internet. Most information is unregulated, and as such there is no guarantee of accuracy.

3) 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.

4) You must not:

   a) use any images, text or material which are copyright-protected, other than in accordance with the terms of the license under which you were permitted to download them;

   b) introduce packet-sniffing or password-detecting software;

   c) seek to gain access to restricted areas of the Company's network;

   d) access or try to access data which you know or ought to know is confidential;

   e) introduce any form of computer virus; nor

   f) carry out any hacking activities.

E) VIRUS PROTECTION PROCEDURES

To prevent the introduction of virus contamination into the software system the following must be observed: -

   a) unauthorised software including public domain software, magazine cover disks/CDs or Internet/World Wide Web downloads must not be used; and

   b) all software must be virus checked using standard testing procedures before being used.

F) USE OF COMPUTER EQUIPMENT

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 be checked and authorised by a member of management or a client's nominated senior member of management before general use will be permitted.

   b) Only authorised staff should have access to the Company's computer equipment.

   c) Only authorised software may be used on any of the Company's 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.

   f) Unauthorised access to the computer facility will result in disciplinary action.

   g) Unauthorised copying and/or removal of computer equipment/software will result in disciplinary action, such actions could lead to dismissal.

G) SYSTEM SECURITY

1) Security of our or our clients' IT systems is of paramount importance. We owe a duty to all our customers/clients to ensure that all of our business transactions are kept confidential. If at any time we need to rely in court on any information which has been stored or processed using our IT systems, it is essential that we are able to

demonstrate the integrity of those systems. Every time you use the system you take responsibility for the security implications of what you are doing.

2) The Company's system or equipment must not be used in any way which may cause damage, or overloading or which may affect its performance or that of the internal or external network.

3) Keep all confidential information secure, use it only for the purposes intended and do not disclose it to any unauthorised third party.

H) PERSONAL TELEPHONE CALLS/ MOBILE PHONES

1) Telephones are essential for our business. Incoming/outgoing personal telephone calls are allowed at the Company's office but should be kept to a minimum. We reserve the right to recharge for excessive personal use.

2) Personal mobile phones should be switched off or 'on silent' during working hours and only used during authorised breaks.

I) MONITORING OF COMMUNICATIONS BY THE COMPANY

1) The Company is ultimately responsible for all business communications but subject to that will, so far as possible and appropriate, respect your privacy and autonomy. The Company may monitor your business communications for reasons which include:

   a) providing evidence of business transactions;

   b) ensuring that our business procedures, policies and contracts with staff are adhered to;

   c) complying with any legal obligations;

   d) monitoring standards of service, staff performance, and for staff training;

   e) preventing or detecting unauthorised use of our communications systems or criminal activities; and

   f) maintaining the effective operation of Company communication systems.

2) From time to time the Company may monitor telephone, e-mail and internet traffic data (i.e. sender, receiver, subject; non-business attachments to e-mail, numbers called and duration of calls; domain names of web sites visited, duration of visits, and non-business files downloaded from the internet) at a network level (but covering both personal and business communications). 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.

3) Sometimes it is necessary for us to access your business communications during your absence, such as when you are away because you are ill or while you are on holiday.

J) DATA PROTECTION

1) As an employee using our communications facilities, you will inevitably be involved in processing personal data for the Company as part of your job. Data protection is about the privacy of individuals and is governed by the General Data Protection Regulation and current Data Protection Acts.

2) Whenever and wherever you are processing personal data for the Company you must keep this secret, confidential and secure, and you must take particular care not to

disclose such data to any other person (whether inside or outside the Company) unless authorised to do so. Do not use any such personal data except as authorised by METAC for the purposes of your job. If in doubt, ask a member of management.

3) The Acts gives every individual the right to see all the information which any data controller holds about them. Bear this in mind when recording personal opinions about someone, whether in an e-mail or otherwise. It is another reason why personal remarks and opinions made should be given responsibly, must be relevant and appropriate as well as accurate and justifiable.

4) For your information, the Act provides that it is a criminal offence to obtain or disclose personal data without the consent of the data controller. "Obtaining" here includes the gathering of personal data by employees at work without the authorisation of the employer. You may be committing this offence if without authority of the Company: you exceed your authority in collecting personal data; you access personal data held by us; or you pass them on to someone else (whether inside or outside the Company).

K) USE OF SOCIAL NETWORKING SITES

Any work-related issue or material that could identify an individual who is a customer/client or work colleague, which could adversely affect the company, a customer/client or our relationship with any customer/client must not be placed on a social networking site. This means that work related matters must not be placed on any such site at any time either during or outside of working hours and includes access via any computer equipment, mobile phone or PDA.

L) CONFIDENTIALITY

Employees are not permitted to register with sites or electronic services in the company's name without the prior permission of their manager. They are not permitted to reveal internal company information to any sites, be it confidential or otherwise, or comment on company matters, even if this is during after-hours or personal use. The company confidentiality policy applies to all electronic communication and data.

M) COMPLIANCE WITH THIS POLICY

1) Failure to comply with this policy may result in disciplinary action being taken against you. If there is anything in this policy that you do not understand, please discuss it with a member of management.

2) Please note that the procedures and policies outlined in this policy, and in any related policy, may be reviewed or changed at any time.