Email Policy

1. Introduction

Skills People Group consists of the following companies.

- *Construction Skills People*
- *C&G Assessments and Training Ltd*
- *Training Futures UK Ltd*

The company is committed to comply with the General Data Protection Regulation (GDPR) which forms part of data protection regime in the UK, together with the new Data Protection Act 2018 (DPA 2018) and the main provisions that apply, like GDPR, from the 25th May 2018.

2. Overview

A common method for sharing information is by email. By necessity the TO, FROM, DATE and SUBJECT fields are transmitted in plain text and may be accessed by any unintended recipient or third-party who intercepts the communication. Without additional encryption and/or password protection in place, the body of any attachments will also be accessible to any unintended recipient or third party who intercepts the communication. To achieve the maximum guarantee the encryption key or password is communicated using a different method, e.g. by disclosing the password over the telephone or by text message.

Personal data can also be at risk if an individual gains unauthorised access to the email server or online account, storing emails which have been read or waiting to be read.

The choice of password securing the server or email is similarly important for the security of the system.

3. Purpose

The purpose of this policy is to detail the company's usage guidelines for the email system. This policy will enable the company to reduce the risk of an email-related security incident, foster good business communications both internally and externally, and provide for consistent and professional application of the company's email communications.

4. Scope

The scope of this policy includes the company's email system in its entirety, including desktop and/or web-based email applications, server-side applications, email relays, and associated hardware. It covers all electronic mail sent from the system, as well as any external email accounts accessed from the company network.

5. Use of Company Email Systems

Users are asked to exercise common sense when sending or receiving email from company accounts. Additionally, the following applies to the proper use of the company email system.

5.1 Sending Email

When using a company email account, email must be addressed and sent carefully. Users should keep in mind that the company loses any control of email once it is sent external to the company network. Users must take extreme care when typing in addresses, particularly when email address auto-complete features are enabled; using the "reply all" function; or using distribution lists to avoid inadvertent information disclosure to an unintended recipient.

Information communicated within an email must be adequate, relevant and limited to what is necessary in relation to its purpose.

Attachments containing 'personal data' must be encrypted or password protected as a minimum requirement. The encryption key or password must be communicated using a different method of communication i.e. disclose the password over the telephone or by text.

5.2 Business Communications and Email

The company uses email as an important communication medium for business operations. Users of the corporate email system are expected to check and respond to email in a consistent and timely manner during business hours.

Additionally, users are asked to recognise that email sent from a company account reflects on the company, and, as such, email must be used with professionalism and courtesy.

The sending of unsolicited email (SPAM) is strictly prohibited.

5.3 Personal Use and General Guidelines

Personal usage of the company email systems is prohibited. Users should use corporate email systems for business communications only.

The following is never permitted:

- Spamming, harassment, communicating threats, solicitations, chain letters, or pyramid schemes.

This list is not exhaustive but is included to provide a frame of reference for types of activities that are prohibited:

- The user is prohibited from forging email header information or attempting to impersonate another person.
- Email is an insecure method of communication, and thus information that is considered confidential or proprietary to the company may not be sent via email, regardless of the recipient, without proper encryption.
- It is company policy not to open email attachments from unknown senders, or when such attachments are unexpected.
- Email systems were not designed to transfer large files and as such emails should not contain attachments of excessive file size.

**Note that the topics above may be covered in more detail in other sections of this policy*.

5.4 Email Signature

An email signature (contact information appended to the bottom of each outgoing email) is required for all emails sent from the company email system. Email signatures are set up by the System Administrator, MCI through the approval of your line manager.

At a minimum the signature should include the user's:

- *Job title*
- *Company name*
- *Telephone number(s)*
- *URL for corporate website*

Email signatures may not include photographs or personal messages (political, humorous, etc.)

5.5 Auto-Responders

The company requires the use of an auto-responder if the user will be out of the office for an entire business day or more. The auto-response should notify the sender that the user is out of the office, the date of the user's return, and who the sender should contact if immediate assistance is required.

5.6 Opening Attachments

Users must use care when opening email attachments. Viruses, Trojans, and other malware can be easily delivered as an email attachment. Users should:

- × Never open unexpected email attachments.
- × Never open email attachments from unknown sources.
- × Never click links within email messages unless he or she is certain of the link's safety. It is often best to copy and paste the link into your web browser, or retype the URL, as specially-formatted emails can hide a malicious URL.

The company may use methods to block what it considers to be dangerous or emails or strip potentially harmful email attachments as it deems necessary.

5.7 Monitoring and Privacy

Users should expect no privacy when using the corporate network or company resources. Such use may include but is not limited to: transmission and storage of files, data, and messages. The company reserves the right to monitor all use of the computer network. To ensure compliance with company policies this may include the interception and review of any emails, or other messages sent or received, inspection of data stored on personal file directories, hard disks, and removable media.

5.8 Company Ownership of Email

Users should be advised that the company owns and maintains all legal rights to its email systems and network, and thus any email passing through these systems is owned by the company and it may be subject to use for purposes not be anticipated by the user. Keep in mind that email may be backed up, otherwise copied, retained, or used for legal, disciplinary, or other reasons. Additionally, the user should be advised that email sent to or from certain public or governmental entities may be considered public record.

5.9 Contents of Received Emails

Users must understand that the company has little control over the contents of inbound email, and that this email may contain material that the user finds offensive. If unsolicited email becomes a problem, the company may attempt to reduce the amount of this email that the users receive, however no solution will be 100 percent effective. The best course of action is to not open emails that, in the user's opinion, seem suspicious. If the user is particularly concerned about an email, or believes that it contains illegal content, he or she should notify their line manager.

5.10 Access to Email from Mobile Phones

Many mobile phones or other devices, often called smartphones, provide the capability to send and receive email. This can present security issues, particularly relating to the storage of email, which may contain sensitive data, on the phone. Users are not to access, or attempt to access, the company's email system from a mobile phone without the permission of his or her line manager.

Note that this section does not apply if the company provides the phone and mobile email access as part of its remote access plan. In this case, permission is implied. Refer to the Mobile Device Policy for more information.

5.11 Access to Email from Mobile Phones

Any specific regulations (industry, governmental, legal, etc.) relating to the company's use or retention of email communications must be listed here or appended to this policy.

6. External and/or Personal Email Accounts

The company recognise that users may have personal email accounts in addition to their company-provided account. The following sections apply to non-company provided email accounts:

6.1 Use for Company Business

Users must use the corporate email system for all business-related email. Users are prohibited from sending business email from a non-company-provided email account.

6.2 Access from the Company Network

Users are prohibited from accessing external or personal email accounts from the corporate network.

6.3 Use for Personal Reasons

Users are required to use a non-company-provided (personal) email account for all non-business communications. The corporate email system is for corporate communications only. Users must follow applicable policies regarding the access of non-company-provided accounts from the company network.

7. Confidential Data and Email

The following sections relate to confidential data and email:

7.1 Passwords

As with any company passwords, passwords used to access email accounts must be kept confidential and used in adherence with the Password Policy. At the discretion of the System Administrator, MCI the company may further secure email with certificates, two factor authentications, or another security mechanism.

7.2 Emailing Confidential Data

Email is an insecure means of communication. should think of email as they would a postcard, which, like an email, can be intercepted and read on the way to its intended recipient.

The company require, the encryption of any email which contains confidential information, this is particularly important when the email is sent to a recipient external to the company.

Refer to 5.1 for safe information transfer requirements.

Further guidance on the treatment of confidential information exists in the company's Data Protection Policy. If information contained in the Data Protection Policy conflicts with this policy, the Data Protection Policy will apply.

8. Company Administration of Email

The company will use its best effort to administer the company's email system in a manner that allows the user to both be productive whilst working as well as reduce the risk of an email-related security incident.

8.1 Filtering of Email

A good way to mitigate risk from email is to filter it before it reaches the user so that the user receives only safe, business-related messages. For this reason, the company will filter email at the Internet gateway and/or the mail server, to filter out spam, viruses, or other messages that may be deemed A) contrary to this policy, or B) a potential risk to the company's IT security. No method of email filtering is 100 percent effective, so the user is asked additionally to be cognisant of this policy and use common sense when opening emails.

Additionally, many email, and/or anti-malware programs will identify and quarantine emails that it deems suspicious. This functionality may or may not be used at the discretion of the System Administrator.

8.2 Email Disclaimers

The use of an email disclaimer is an important component in the company's risk reduction efforts. The company require the use of the following email disclaimer at the bottom of every outgoing email.

This email and its attachments may be confidential and are intended solely for the use of the individual to whom it is addressed. Any views or opinions expressed are solely those of the author and do not necessarily represent those of Skills People Group Ltd. If you are not the intended recipient of this email and its attachments, you must take no action based upon them, nor must you copy or show them to anyone. Please contact the sender if you believe you have received this email in error. This e-mail has been created in the knowledge that e-mail is not necessarily a secure communications medium. We advise that you understand and observe this lack of security when e-mailing us. Although we have taken steps to ensure that this e-mail and attachments are free from any virus, responsibility for any loss or cost arising from its transmission is hereby excluded.

8.3 Email Deletion

Users are encouraged to delete emails periodically when the email is no longer needed for business purposes. The goal of this policy is to keep the size of the user's email account manageable and reduce the burden on the company to store and backup unnecessary email messages.

However, users are strictly forbidden from deleting email to hide a violation of this or another company policy. Further, emails must not be deleted when there is an active investigation or litigation where that email may be relevant.

8.4 Retention and Backup

Email should be retained and backed up in accordance with the applicable policies.

Unless otherwise indicated, for the purposes of backup and retention, email should be considered operational data.

8.5 Address Format

Email addresses must be constructed in a standard format to maintain consistency across the company.

8.6 Account Activation

Email accounts will be set up for each user determined to have a business need to send and receive company email.

8.7 Account Termination

When a user leaves the company, or his or her email access is officially terminated for another reason, the company will disable the user's access to the account by password change, disabling the account, or another method. The company is under no obligation to block the account from receiving email and may continue to forward inbound email sent to that account to another user or set up an auto-response to notify the sender that the user is no longer employed by the company.

8.8 Storage Limits

As part of the email service, email storage may be provided on company servers or other devices. The email account storage size must be limited to what is reasonable for each employee, at the determination of the System Administrator. Storage limits may vary by employee or position within the company.

9. Prohibited Actions

The following actions shall constitute unacceptable use of the corporate email system. This list is not exhaustive but is included to provide a frame of reference for types of activities that are deemed unacceptable. The user may not use the corporate email system to:

Send any information that is illegal under applicable laws.

- Access another user's email account without A) the knowledge or permission of that user – which should only occur in extreme circumstances, or B) the approval of company executives in the case of an investigation, or C) when such access constitutes a function of the employee's normal job responsibilities.
- Send any emails that may cause embarrassment, damage to reputation, or other harm to the company.
- Disseminate defamatory, discriminatory, vilifying, sexist, racist, abusive, rude, harassing, annoying, insulting, threatening, obscene or otherwise inappropriate messages or media.
- Send emails that cause disruption to the workplace environment or create a hostile workplace. This includes sending emails that are intentionally inflammatory, or that include information not conducive to a professional working atmosphere.
- Make fraudulent offers for products or services.
- Attempt to impersonate another person or forge an email header.
- Send spam, solicitations, chain letters, or pyramid schemes.
- Knowingly misrepresent the company's capabilities, business practices, warranties, pricing, or policies.
- Conduct non-company-related business.

The company may take steps to report and prosecute violations of this policy, in accordance with company standards and applicable laws.

9.1 Data Breach

Data can leave the network in several ways. Often this occurs unintentionally by a user with good intentions. For this reason, email poses a challenge to the company's control of its data.

Unauthorised emailing of company data, confidential or otherwise, to external email accounts for saving this data external to company systems is prohibited. If a user needs access to information from external systems (such as from home or while traveling), that user should notify their line manager rather than emailing the data to a personal account or otherwise removing it from company systems.

*Incidents or data breaches must be reported to the Data Protection Officer immediately.

9.2 Sending Large Emails

Email systems were not designed to transfer large files and as such emails should not contain attachments of excessive file size. The company asks that the user limit email attachments to 10Mb or less.

The user is further asked to recognise the additive effect of large email attachments when sent to multiple recipients and use restraint when sending large files to more than one person.

10. Applicability of Other Policies

This document is part of the company's cohesive set of security policies. Other policies may apply to the topics covered in this document and as such the applicable policies should be reviewed as needed.

11. Incident Reporting

Data Protection incidents must be reported immediately to the Data Protection Officer.
The Data Protection Officer is Amanda Wareham
or alternatively you can contact Julie Lawton on 07519 109896 or 01246 589459

12. Enforcement

Violations to this policy may result in disciplinary action, which may include suspension, restriction of access, or more severe penalties up to and including termination of employment. Where illegal activities or theft of company property (physical or intellectual) are suspected, the company may report such activities to the applicable authorities.

This policy has been produced using guidance within the 'Guide to General Data Protection Regulation' (GDPR) located on the Information Commissioners Office (ICO) website:
https://ico.org.uk/for-organisations/guide-to-data-protection/encryption/scenarios/sending-personal-data-by-email/

Document Control

Date of change	Version	Overview of amendment	Amended by / Job title	Approved by	Approval date
29-02-16	1	Policy created	MCI & A Warham (Operations Director)	A Warham	29-02-16
26-05-17	2	Policy revised and cover sheet added	MCI & A Warham (Director)	A Warham	26-05-17
10-09-18	3	Policy revised to bring in line with GDPR	Julie Lawton (Quality Manager)	A Warham	16-10-18