



Acceptable Email Usage Policy (AEUP).

Copyright of Information and Documents

The copyright of this document is vested in [Company Name] and is issued in confidence only for the purpose for which it is supplied.

©[Company Name][Year]

Document Ownership

This document is the property of [Company Name] and is issued for the information of such persons who have a need to know its contents in the course of their official duties. Any person finding this document is requested to inform [Company Name] [Telephone Number] and return it safely to the following address stating the circumstances in which it was discovered:

[Company Name]
[Line 1 Address]
[Line 2 Address]
[Line 3 Address]
[Postcode]

Document Reference & Author Information

Document Reference : [Document Reference Number & Version]
Date : [Document Issue Date]
Author : [Name & Position]
Owner : [Name & Position]
CDS Target Level : [CDS Level 1]

Table of Contents

- Copyright of Information and Documents 1
- Document Ownership..... 1
- Document Reference & Author Information..... 1
- Document Version Information.....2
- Links & Dependencies2
- Register of Applicable Legislation [UK Legislation supplied for information]2
- Compliance with Corporate Policies.....2
- 1. Purpose3
- 2. Privacy.....3
- 3. Monitoring.....3
- 4. Mandatory Requirements.....3
- 5. Data Security5
- 6. Physical Security.....5
- 7. Encryption.....5
- 8. Copyright6
- Issuing Person & Recipient Acknowledgement Statement6

Document Version Information

Version	Changes	Date
1.0	Initial Draft	

Links & Dependencies

Document Title	Reference	Date

Register of Applicable Legislation [UK Legislation supplied for information]

Document Title	Reference	Date
Computer Misuse Act	CMA	1990
Data Protection Act	DPA	1998
Human Rights Act	HRA	1998
Copyright, Designs & Patents Act	CDP	1998
Freedom of Information Act	FOI	2000
Regulation of Investigatory Powers Act	RIPA	2000
Telecommunications Lawful Business Practice (Interception of Communications Regulations)	TLBP(ICR)	2000
Communications Act	TCA	2003

Compliance with Corporate Policies

Document Title	Reference	Date

Abbreviations

Terms & Abbreviations	Explanation or Expansion
Authorised access	Given authority by the data custodian to access business information or given authority to access areas controlled by the business.
Authorised user account	User account provided by a system administrator for use on business systems.
Business	Sole proprietors, partnerships, companies & corporations operating information systems.
Business systems	Any company owned, rented, leased asset capable of carrying or transmitting electronic data.
Chain letter	Mail to induce the recipient to copy the letter then pass it on to as many recipients as possible.
Digest	A format of distribution of electronic messages placed together as a single unit.
Mb	Measure of Data Size where 1 Megabyte (Mb) = 1024 Kilobytes (Kb) = 1024000 Bytes.
RSS	Really Simple Syndication used to publish & distribute frequently



	updated works such as news.
Spam	Unsolicited bulk messages distributed indiscriminately.

1. Purpose

The purpose of this document is to convey the ethos of [Company Name] and what the company deems as appropriate in the electronic business communications of its employees.

This policy is to ensure that all employees representing the company through electronic and other communications have read, understood and agreed to comply with all requirements which govern their usage which includes all associated liabilities.

2. Privacy

All systems are subject to monitoring at the company's discretion and there should be no expectation of privacy when using business systems.

3. Monitoring

Monitoring of email communications may be undertaken for purposes which can include cost analysis, resource allocation, management of information resources and detecting usage which might indicate employees may be violating policies or engaging in illegal activities. The capability, frequency and duration of any monitoring are subject to change without notice to the employees.

In accepting an authorised email account for use on business systems:

- a. The employee is deemed to have been provided with all relevant policy documentation governing the acceptable use of their account.
- b. The employee has effectively agreed to be legally bound by [Company Name] terms and conditions of usage of their email account which has been provided for business usage.

Any breach of the following items may result in disciplinary action which can vary depending on the nature and severity of the incident.

Any records presented as part of any disciplinary actions will conclude that the user had full knowledge and responsibility for their actions, and, continued both intentionally and voluntarily to breach these requirements.

4. Mandatory Requirements

[Regardless of other statements deemed appropriate by the organization, to be compliant with CDS requirements the policy must contain the following mandatory elements]

- a. Authorised employees are deemed responsible for any and all actions attributed to their email account(s) as provided by the company unless they have previously notified their account as compromised.
- b. Any email account provided by the company is to be used solely for business purposes.

[A 'fair use' statement may be included here to allow employees to use their business email account for personal purposes, but will attract a management overhead in defining for which purposes and at what times personal access would be allowed, and, how the management of such would be enforced.]

- c. Personal email accounts such as Hotmail, Gmail etc are / are not* permitted to be accessed via business IT systems. *[The decision on allowing this type of access rests with the organization, but there must be a positive statement on the use of personal email – the recommended position is to disallow personal email accounts.]*



d. The following types of email are considered to be unacceptable:

[A list should be placed here – the types of email that the organization should consider listing include emails which are inflammatory or derogatory, espouse extreme political, religious or racial views, encourage violent or illegal activities, breach legislation relating to sex, race, age or religious discrimination, or disseminate offensive or pornographic material.]

e. Emails & attachments can contain hostile code, scripts and viruses or other programs that could compromise, impair or destroy data on [Company Name] business systems. Where an email user has any doubt as to contents or attachments received to their email they are instructed not to open, download or forward the email or attachment, and, report the suspect email to their systems administrator.

f. Employees must not register their business email account on any site which does not pertain to the company's business or functions. Subscriptions to information & news sites should not be made unless directly related to the role of the employee, and, where applicable should only be such as to receive information which has been bound as a digest.

g. Where there is any doubt as to the relevance of the subject matter of sites which provide newsletters or RSS feeds to a business email account, written authority should be obtained from [Senior Manager Position or Name].

h. Employees are to report any unsolicited or spam email to the systems administrator for appropriate action to filter, restrict, block and or investigate, based on the merits of the occurrence(s).

i. In the event that excessive or mail deemed by the company as irrelevant/erroneous, the system administrator will, without notice, block future incoming mail from specific sources to that employee's email account.

j. In the event that unsolicited or spam mail is being received by the company and/or an employee's email account, the system administrator will, without notice, block future incoming mail from specific sources to the company and employee's email accounts.

k. With the exception of the following designated groups : [eg. Helpdesk, Support, Sales, Marketing], employees are advised not to open nor respond nor unsubscribe to unsolicited emails, as they may contain hostile code or redirect the employee to a hostile website.

l. Where groups [eg. Helpdesk, Support, Sales, Marketing] are required to receive unsolicited email as part of their business function, due care and diligence should be made when ascertaining the legitimacy of an email and its contents.

m. Should any employee be in any doubt as to the contents or legitimacy of a received email, they are to seek guidance from their line manager or the systems administrator. In such cases the email in question must not be forwarded unless specifically requested to do so by the systems administrator.

n. Employees must be aware that the nature, type, punctuation & placement of words and the construction of sentences can impact on the messages being conveyed. Due care must be taken to avoid sending emails which could be perceived as being inflammatory, abusive, discriminatory or derogatory to any group or individual, or which may portray the company negatively.

o. Employees are advised that both incoming and outgoing attachments are subject to restrictions both in terms of size & content. Due to the impracticality of receiving & sending emails larger the 10Mb, employees are advised to seek alternative methods of communicating this volume of data. Where there is a continual business requirement to regularly receive/send such volumes of data, this should be identified as a business case to accommodate such movement through managerial approval. Any subsequent approvals and guidance will be issued in a new release of this document.



[Optional : A list of file extensions which will be automatically blocked from the business systems.]

- p. The transmission by email of information relating to contracts, finances or strategy is only authorized for those personnel directly involved in those particular activities.

[Depending on the size of the organization this may not be appropriate, but a positive statement as to the sending of business sensitive information must be made.]

- q. When sending sensitive personal information, the data is to be encrypted using *[insert organizations preferred product here]* and attached to an email. Encryption keys will be provided by IT on authority from *[name of management approver]*; keys will only be exchanged with 3rd parties who are approved to receive the information.
- r. The organization is bound by national and international law and will co-operate with the police where required or requested to do so. This might include providing information on users' activities, surrender of IT assets for examination, or details of the contents of emails.

5. Data Security

Employees will be prompted & required to change their passwords at regular intervals which will force a minimum level of length & complexity.

No written record of a password should be stored by the employee. In the event that the password is unavailable, the employee must obtain a new password from the systems administrator.

In the event that employees need to move away from the business systems being used, they are required to ensure that their business email is inaccessible by unauthorized persons by either password locking their session, or logging off the business system.

6. Physical Security

Employees with portable business assets must take reasonable precautions to ensure that the asset is not lost nor the data held on that asset compromised. When away from business premises, the business asset should always be under direct control of the employee or secured in a location not readily visible by unauthorised persons.

Overnight & weekend storage of portable business assets must be secured in locked units to prevent unauthorised physical access.

7. Encryption

Only file protection or encryption software provided by the business is to be used on business systems. Any non-compliant data files will be treated as hostile and removed without notice and may be subject to disciplinary action.

Where usage of encryption technologies is suspected of being used in an unauthorised manner the employee's user account will be immediately suspended pending an investigation.

The business reserves all rights to immediately access any data file held on its systems. Where access through the provision of user/employee held passwords are unavailable, the business will undertake whatever measures deemed necessary to access the data held.



8. Copyright

Where information obtained from Internet usage is to be reused or displayed, due diligence must be observed in compliance with ownership and copyright law. Any information obtained from internet sources and reused must be properly referenced with its origin.

Issuing Person & Recipient Acknowledgement Statement

Document Issuer Name		
Printed & Signed	Position/Role/Group	Date
Recipient Acknowledgement Statement		
"I [<i>Recipient Name</i>] fully understand, accept and agree to be legally bound by the contents of this policy which forms part of my terms and conditions of employment and may be subject to amendment. I am fully aware and accept that [<i>Company Name</i>] have a duty of care for legal compliance & to maintain business continuity, and, will take any unreserved actions deemed necessary to ensure the protection of data held or accessed on or by its business systems."		
Document Recipient Name		
Printed & Signed	Position/Role/Group	Date