



Acceptable Internet Usage Policy (AIUP).

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 & Dependencies	2
Register of Applicable Legislation [UK Legislation supplied for information]	2
Compliance with Corporate Policies.....	2
1. Purpose	3
2. Privacy.....	3
3. Monitoring.....	3
4. Mandatory Requirements.....	3
5. Data Security	Error! Bookmark not defined. 2
6. Physical Security.....	Error! Bookmark not defined. 2
7. Encryption.....	Error! Bookmark not defined. 2
8. Copyright	4
Issuing Person & Recipient Acknowledgement Statement	4

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.



1. Purpose

The purpose of this document is to convey the ethos of [Company Name] and what is deemed appropriate in the use of their business facilities to access the internet.

This policy is to ensure that all users accessing the internet using a business supplied connection 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 business systems may be undertaken for purposes which can include cost analysis, resource allocation, management of information resources and detecting patterns of use which might indicate users 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 user account for use on business systems:

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

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.

[include details of how monitoring will be carried out, i.e. automated by software, manually by the IT staff.]

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 users of business systems are deemed responsible for any and all actions attributed to their accounts provided by the company.
- b. Any software or hardware capable of providing or accessing the Internet is to be used solely for business purposes.

[A 'fair use' statement must be included here as to whether or not the organization allows employees to access the internet for personal purposes, including the use of webmail, instant messaging and social networking sites.]

- c. Internet Access must not be used to access or interact with any information, images, sites or feeds, which are, or potentially may be, obscene, abusive, pornographic, discriminatory, derogatory to any group or individual, or which may be either unlawful or illegal.

[Insert Company Logo]

[Company Name]



[Specific statements must be made regarding accessing sites featuring pornography, violence, or promotion or support of illegal activities. Statements must also be made on the use of shopping and gambling sites, file sharing sites and sites which include the topics of war and weapons, religious views, or graphic medical content. The decision to allow or deny rests with the organization, but a statement of their decision must be recorded in this acceptable use policy.]

- d. Should a user have any doubt as to the contents or legality of data which might be provided when accessing a site or internet link, they are not to continue to attempt access to that site or link.
- e. Sites or links which a user thinks may contravene sub-paragraph c above are to report their findings to the system administrator.
- f. 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' web browsing activities or surrender of IT assets for examination.

5. 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	Date
Recipient Acknowledgement Statement		
"I [Recipient Name] 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 [Company Name] 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	Date