Acceptable Use Policy

PHX026

Contents

Policy Statement

Phoenix seeks to promote, sell, and facilitate the proper and extensive use of information and communication technology. This requires responsible and legal use of the technologies and facilities made available to all employees, partners and contracted third parties sharing in the responsibility to ensure that Phoenix meets this objective.

Phoenix systems, services and facilities are provided to enable employees and other authorised individuals to perform their jobs effectively and efficiently. All normal use of these systems in pursuit of Phoenix business within an employee's authority to act is allowed however unauthorised or illegal activity is not allowed.

Purpose

This policy establishes acceptable and proper use of the company's systems with the overall aim of protecting the rights and privacy of all employees and the integrity and reputation of Phoenix.

Phoenix provides devices, networks, and other electronic information systems to meet the objectives of the business and must manage these responsibly to maintain the confidentiality, integrity, and availability of its information assets. This policy requires the users of information assets to comply with Phoenix policies and to protect the company against any information security breach, information loss and potential legal issues.

This Acceptable Use Policy is intended to provide a framework for the correct use of the company's resources and applies to all IT, telecommunication and networking facilities provided by the Phoenix.

Limited and reasonable personal use of Phoenix systems by employees is allowed provided that it is not excessive and does not:

- interfere with normal work or the work of others
- involve more than minimal amounts of working time
- involve Phoenix in significant expense
- expose the company to legal action or risk bringing Phoenix into disrepute
- expose the company or its customers to any undue risk (security, privacy, reputation)
- relate to running a private business

This policy applies to all employees of Phoenix. The principles of the policy will also be applied, as far as is reasonably practicable, to non-employees working at the Phoenix offices and making use of company's systems.

The policy sets the minimum standards of IT acceptable use. Breaches of the policy will be dealt with under the disciplinary procedure or if appropriate the Fraud Bribery and Money Laundering Policy.

Principles and Scope

Phoenix relies on its systems and communications facilities to carry out its business. All these facilities can be put at risk through improper or ill-informed use and result in consequences which may be damaging to individuals, the business, the Phoenix brand, and its reputation.

The policy aims to provide clear guidance to all employees concerning the use of Phoenix systems and communications facilities. It provides a framework to:

- protect company data
- enable employees to use Phoenix facilities with security and confidence
- help maintain the security, integrity, and performance of Phoenix systems
- minimise both Phoenix and individual users' exposure to possible legal action arising from unauthorised use of the systems
- help ensure that Phoenix can demonstrate effective and appropriate use of resources
- set the minimum standard for acceptable use across all of Phoenix systems

It is the responsibility of Phoenix to ensure that employees have access to this policy, both on joining and during their employment. It is each employee's responsibility to read, make themselves fully familiar with and abide by the policy and other relevant company policies.

The policy covers use of all IT systems and facilities provided either directly or indirectly by Phoenix or used to conduct the company’s business, whether accessed from the company offices or remotely, in particular:

- the internet
- electronic communications (in all forms) for example e-mail, social media used for business related communication, etc
- file sharing by whatever means
- devices (e.g., laptops, printers, mobile devices etc.) and servers
- communications equipment (e.g., telephones (land-line and mobiles) plus video conferencing)

Sensitive or personal information must be appropriately protected in line with Phoenix policies and with the UK General Data Protection Regulation (UK GDPR)Any activity that falls outside acceptable use as defined by this policy and aligned Information Security policies may result in disciplinary action (see Phoenix Disciplinary Procedure).

Where the activity is deemed to amount to gross misconduct, this will normally lead to instant dismissal. When and if relevant the Phoenix Fraud Bribery and Money Laundering Policy may also be invoked.

Contractors will be made aware, by email of any restrictions/guidance before they have access to Phoenix systems and services.

Private/Personal Use of Systems, Services & Facilities

Phoenix employees are allowed limited and reasonable personal use of the company systems, services, and facilities provided that such use does not:

- interfere with their (or others') work
- involve more than minimal amounts of working time
- incur any significant expense for Phoenix or tie up a significant amount of resource

Personal use should be limited to non-working time e.g. at lunchtime, before/after normal working hours. Very limited, occasional personal use during normal working time will be tolerated (e.g. to respond briefly to an incoming personal e-mail or telephone call or to deal with a non-work-related emergency).

Spending significant amounts of time however making personal use of the internet, e-mail, communication equipment is not acceptable and if repeated will lead to disciplinary action.

Before undertaking personal use, employees should ask themselves the following questions.

- Would the actions be considered unacceptable if viewed by a member of the management?
- Would managers, auditors or others in similar positions call into question the cost effectiveness of use of work time or use of company systems and facilities?
- Will personal use have a negative impact upon the work of colleagues (e.g. in terms of their motivation and morale)?
- Could personal use bring Phoenix directly or indirectly into disrepute?
- Personal use should not be undertaken if the answer to any of these questions is yes

Phoenix blocks unsuitable website content which is seen as unacceptable for the workplace. These categories are reviewed at regular intervals.

Responsibility for ensuring that any personal use is acceptable rests with the individual. Employees should seek guidance from their manager if they have any doubts concerning the acceptability of their personal use. If any doubt still remains, then that form of personal use should not be undertaken.

Social Media

Phoenix recognises the value of using social media in work related communication. It can be an effective way to respond to enquiries, keep employees and customers informed or to track and respond to matters relating to Phoenix business.

Employees should have their manager's approval before using social media for work related communication and must read and comply with any rules before using social media for Phoenix related work.

Monitoring

Phoenix reserves the right to monitor all communications in line with the Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000. This is also known as the 'Lawful Business Practice' Regulations which provides the legal basis which allows organisations to monitor staff emails and other forms of digital communications, including their use of the Internet while at work.

Phoenix employs monitoring techniques on its systems and services, including e-mail and Internet access, to enable usage trends to be identified and to ensure that these facilities are not being misused.

We continuously monitor through a dedicated internal Security Operations Centre team. We collect network traffic, email and exchange, endpoint protection, Active Directory and accounts, DNS traffic, Discovered SaaS application details, Threat Intelligence data all within a SIEM solution. Alerting rules have been created to be notified of any anomalies found within the data to trigger investigation and triage processes. The team also carry out proactive threat hunting within the collected logs to identify potential misconfigurations or anomalies within systems to prevent attacks before they occur.

Phoenix owns and is responsible for data held on its communications equipment and systems. It reserves the right, as part of any investigations, to inspect the contents of any emails or any other form of communications that are sent or received and of internet sites accessed, for compliance with this policy. This will be done where there are grounds to suspect that use is for unacceptable or illegal activity.

Exceptionally, where there is a defined and valid reason for doing so, the inspection may include items marked 'private' or 'personal'. An individual's e-mail and voice-mail accounts may also be accessed by management when the individual is absent from work to ensure official business matters can be effectively dealt with. Authorisation for such access is given by the relevant Phoenix manager.

Authorisation

Employment grants authorisation to use the core IT facilities at Phoenix.

A username, password and e-mail address are allocated to relevant employees.

Individually allocated usernames, passwords, licence certificates and e-mail addresses are for the exclusive use of the individual to whom they are provided. The user is personally responsible and accountable for all activities carried out under their username.

The password associated with a particular personal username must not be divulged to any other person.

No one may use, or attempt to use, IT resources allocated to another person, except when explicitly authorised by the provider of those resources.

All users must correctly identify themselves at all times. A user must not masquerade as another, withhold their identity or tamper with audit trails. A user must take all reasonable precautions to protect their resources. In particular, passwords used must adhere to current password policy and practice. Advice on what constitutes a good password may be obtained from the Service Desk department. This advice must be followed, failure to do so may be regarded as a breach of this policy.

Privacy

In order to use the IT facilities at Phoenix, a person must first be authorised. Authorisation to use Phoenix services is conditional upon acceptance of this Acceptable Use Policy.

It should be noted that staff who have authorisation to access other employee’s devices must ensure the privacy of those users. Phoenix fully reserves the right to monitor e-mail, telephone and any other electronically-mediated communications, whether stored or in transit, in line with its rights under the Regulation of Investigatory Powers Act (2000). Reasons for such monitoring may include the need to:

- ensure operational effectiveness of services
- prevent or investigate a breach of the law, this policy, or other Phoenix policies
- monitor standards

Staff should be aware that any data stored or transmitted from a company owned device or service may be backed up and would be accessible to the company.

Access to staff files, including electronic mail files or individual IT usage information will not normally be given to another member of staff unless authorised by a Director.

The manager will be informed and consulted prior to action being taken. Such access will normally only be granted in the following circumstances:

- where a breach of the law or a serious breach of this or another Phoenix policy is suspected
- when a documented and lawful request from a law enforcement agency such as the police or security services has been received
- where managers request access to e-mail messages or files for business reasons due to absence
- Phoenix sees staff privacy as desirable but not as an absolute right, therefore staff should not expect to hold or pass on private information, which they would not wish to be seen by members of staff responsible for their day-to-day work
- when a member of staff leaves the company, files which are left behind on any computer system owned by, or managed on behalf of Phoenix, including servers, and including electronic mail files, will be considered to be the property of Phoenix

Behaviour

No person shall jeopardise the integrity, performance, security or reliability of IT equipment, software, data, or other stored information.

The integrity of Phoenix systems is put at risk if users do not take adequate precautions against malicious software, such as viruses and associated malware.

The Service Desk department must ensure that any Phoenix device which is attached to the company network is adequately protected against viruses.

It is the employee’s responsibility that any Bring Your Own Devices must adhere to the above rule.

Phoenix is committed to achieving a working environment which provides equality of opportunity and freedom from discrimination. Distributing material, which is offensive, obscene, or abusive, may be illegal and may also contravene Phoenix codes on harassment or discrimination.

Users of Phoenix IT systems must make themselves familiar with and comply with,. The Harassment Policy.

No user shall interfere or attempt to interfere in any way with information belonging to or material prepared by another user. Similarly no user shall make unauthorised copies of information belonging to another user. The same conventions of privacy should apply to electronically held information as to that held on traditional media such as paper.

Procurement of IT equipment must be undertaken by the approved persons and adhere to Phoenix's current policies relating to such purchases.

Users of services external to Phoenix are expected to abide by any policies, rules and codes of conduct applying to such services. Any breach of such policies, rules and codes of conduct may be regarded as a breach of this Acceptable Use Policy and be dealt with accordingly. This includes social networking sites, blogs, and any other externally hosted services. The use of Phoenix credentials to gain unauthorized access to the facilities of any other organization is similarly prohibited.

All e-mails must utilise the data classification tabs of either Public, Confidential and Strictly Confidential.

Definitions of Acceptable and Unacceptable Usage

Unacceptable Use of Phoenix devices and network resources may be summarised as:

- the retention or propagation of material that is offensive, obscene, or indecent, except in the course of recognised research or teaching that is permitted under UK and international law; propagation will normally be considered to be a much more serious offence

- intellectual property rights infringement, including copyright, trademark, patent, design, and moral rights
- causing annoyance, inconvenience, or needless anxiety to others
- defamation
- unsolicited advertising, often referred to as "spamming"
- sending e-mails that purport to come from an individual other than the person actually sending the message using, e.g., a forged address
- attempts to break into or damage IT systems or data held thereon
- actions or inactions which intentionally, or unintentionally, aid the distribution of viruses or other malicious software
- attempts to access or actions intended to facilitate access to computers for which the individual is not authorised
- using the Phoenix network for unauthenticated access
- excessive personal IT use during working hours
- not storing confidential or internal use data on removable media (SD-card, USB, CD-ROM etc.)
- storing of company and customer secrets (credentials, card details, pin codes etc) outside of the company password management tool

The following activities will normally be considered to be a breach of this policy (potential exceptions should be discussed with the Service Desk department):-

- the downloading, uploading, distribution, or storage of music, video, film, or other material, for which you do not hold a valid licence, or other valid permission from the copyright holder
- the use of peer-to-peer software and related applications to illegally download or share music, video, film, or other material, in contravention of copyright law
- the publication on external websites of unauthorised recordings
- the distribution or storage by any means of pirated software
- the connection of an unauthorised device to the Phoenix network, i.e. one that has not been configured to comply with this policy and any other relevant regulations and guidelines relating to security, IT purchasing policy and acceptable use.
- circumvention of network access control
- monitoring or interception of network traffic without permission
- probing for the security weaknesses of systems by methods such as port-scanning without permission
- associating any device to network access points, including wireless, for which you are not authorised
- non-work-related activities which generate heavy network traffic
- excessive use of resources such as file store, leading to a denial of service to others, especially when compounded by not responding to requests for action
- use of Phoenix owned IT equipment, especially where such activities interfere with others' legitimate use of ICT services
- the deliberate viewing and printing of pornographic images
- the passing on of electronic chain mail
- posting of defamatory comments about the company, staff, or employees on social networking sites
- the creation of web-based content, portraying official Phoenix business without express permission or responsibility

- the use of Phoenix business data or mailing lists for non-work-related purposes
- the use of CDs, DVDs, and other storage devices for copying unlicensed copyright software, music, etc.
- the copying of other people's web site, or other, material without the express permission of the copyright holder
- excessive use of data on mobile phones that costs the company excess fees.

It should be noted that individuals may be held responsible for the retention of attachment material that they have received, via e-mail that they have read. Similarly, opening an attachment, received via unsolicited e-mail, especially if clearly unrelated to work, which leads to widespread virus infection, may result in disciplinary action being taken. Disciplinary action may also be taken if casual or non-work-related activity results in significant problems being caused for ICT systems or services, arising for example from browsing non-work-related websites or the downloading of software containing malicious content.

Acceptable Use may include:

- personal e-mail and recreational use of Internet services, as long as these are in keeping with the framework defined in this policy document, do not interfere with one's duties, responsibilities or the work of others and not used to transmit company or customer data
- advertising via electronic notice boards, intended for this purpose, or via other Phoenix approved mechanisms

Such use must not be regarded as an absolute right and may be withdrawn if abused or if the user is subject to a disciplinary procedure.

Legal Constraints

Any software or hard copy of data or information which is not generated by the user personally and which may become available through the use of Phoenix IT or communications resources shall not be copied or used without permission of the company or the copyright owner.

Software information provided by Phoenix may only be used as part of the user's role as an employee of the company. The user must abide by all the licensing agreements for software entered into by Phoenix with other parties, noting that the right to use any such software outside the company will cease when an individual leaves.

Any software licensed under a Phoenix agreement must be removed from a privately owned computer upon leaving the company. This is as well as all Phoenix owned data, such as documents and spreadsheets.

When a computer ceases to be owned by the company, all data and software must be removed from it, in accordance with Phoenix Software's policies.

In the case of private work and other personal use of IT facilities, Phoenix will not accept any liability for loss, damage, injury, or expense that may result.

The user must comply with all relevant legislation including the Computer Misuse Act 1990

General Requirements

All employees are responsible for exercising good judgment regarding appropriate use of Phoenix resources in accordance with the company's policies, standards, and guidelines. Phoenix resources may not be used for any unlawful or prohibited purpose.

For security, compliance and maintenance purposes, authorised personnel may monitor and audit equipment, systems, and network. Devices that interfere with other devices or users on the Phoenix network may be disconnected. Information security prohibits actively blocking authorised audit scans. Firewalls and other blocking technologies must permit access to the scan sources.

Phoenix adopts an orderly desk policy to ensure that documentation is not visible to unauthorised personnel.

Where a whiteboard is available in a public meeting room it is important it is left clean after use as stated on the corresponding notice. This is to ensure business information is not available to unauthorised personnel.

Security of System Accounts

All employees are responsible for the security of data, accounts, and systems under their control. Passwords must be kept secure, and employees will not share account or password information with anyone, including other personnel, family, or friends. Providing access to another individual, either deliberately or through failure to secure its access, is a violation of this policy.

All employees must maintain system-level and user-level passwords in accordance with Phoenix password procedures. Guidance to meet with this requirement can be attained from the Service Desk team.

Storage of company and customer secrets (credentials, card details, pin codes etc) must be held within the company password management tool

Employees must ensure through legal or technical means that work related data remains within the control of Phoenix at all times. Conducting company business that results in the storage of work-related data on personal or non-Phoenix controlled environments, including devices maintained by a third party with whom Phoenix does not have a contractual agreement, is prohibited. This specifically prohibits the use of an e-mail account that is not provided by Phoenix, or its customer and partners, for company business.

IT Assets

All employees are responsible for ensuring the appropriate protection of assigned Phoenix assets. Any theft of Phoenix assets must be reported immediately to a Senior Manager or Director.

All devices must be secured with a password-protected screensaver with the automatic activation feature set to 10 minutes or less. Employees are required to lock the screen or log off when the device is unattended.

Devices that connect to the Phoenix network must comply with the Phoenix Software Access Control Policy and do not interfere with corporate device management or security system software, including, but not limited to, antivirus, device management or security system.

Mobile devices must not be left unattended in vehicles and must be transported out of sight.

Electronic Communications

The following are strictly prohibited:

- inappropriate use of communication vehicles and equipment, including, but not limited to, supporting illegal activities, and procuring or transmitting material that violates Phoenix policies or the safeguarding of confidential or work-related data
- sending Spam via e-mail, text messages, instant messages, voice mail or other forms of electronic communication
- forging, misrepresenting, obscuring, suppressing, or replacing a user identity on any electronic communication to mislead the recipient about the sender
- posting the same or similar non-business-related messages to large numbers of newsgroups
- use of a Phoenix e-mail or IP address to engage in conduct that violates Phoenix policies or guidelines. The user must exercise good judgment to avoid misrepresenting or exceeding your authority in representing the opinion of the company

Enforcement

Phoenix employees found to have violated this policy may be subject to disciplinary action, up to and including termination of employment. A violation of this policy by a contracted third party, partner/contractor or vendor may result in the termination of their contract or assignment with Phoenix.

Version Control

Author	Version	Date	Description
ISC	1.0	01/07/2015	Original Document
ISC	2.0	17/09/2018	Amendments following annual review
ISC	3.0	10/10/2019	Amendments following annual review
ISC	3.0	09/09/2021	Annual review – no change
ISC	4.0	07/12/2022	Amendments following annual review

Document Approval

Name	Version	Date	Position
Sam Mudd	1.0	01/07/2015	Managing Director
Sam Mudd	2.0	17/09/2018	Managing Director
Sam Mudd	3.0	10/10/2019	Managing Director
Sam Mudd	3.0	09/09/2021	Managing Director
Clare Metcalfe	4.0	07/12/2022	Operations Director

Signed: Clare Metcalfe Clare Metcalfe, Operations Director

Dated: 07/12/2022