**ICT, MEDIA & MARKETING POLICY – PP09**

1. **INTRODUCTION**

As with any other modern business, Information and Communication, Technology (ICT), is fundamental to the efficient running of Phoenix Support. As a company Phoenix Support is committed to making the best use of the ICT systems we have in place and to a program of continuing expansion of the use of ICT throughout its services, with this goes the progressive use and development of media and marketing.

1. **POLICY STATEMENT**

It is the policy of Phoenix Support to move forward towards a fully protected electronic storage system, with this in mind we will develop our processes to incorporate the development of this. We will ensure investment into the growth of our media capacity and the production of quality marketing to provide external information to develop our business.

1. **DEFINITION**

This policy consists of a set of rules and guidelines that are to be followed by Phoenix Support employees in order to ensure that our ICT systems remain stable and secure. We aim to define what we cover as media, and what material we can offer and develop for the promotion of our business

1. **PURPOSE**

The misuse of ICT systems can have serious consequences for the security, efficiency and reputation of Phoenix Support. This Policy is provided to minimise the risk of any harm to the company, its employees or service users.

1. **CONTEXT**

Phoenix Support and its employees are bound by the provisions of the Computer Misuse Act 1990 and the GDPR 2018. The company has a responsibility to ensure that its employees abide by these acts, as with other advertising material various legislation will apply to which Phoenix Support will abide

1. **IMPLEMENTATION**

|  |  |
| --- | --- |
| **CONTENTS OF SECTION** | |
|  | **ACCEPTABLE USE OF COMPANY IT RESOURCES** |
|  | **COMPUTER SYSTEMS POLICY** |
|  | **SYSTEM INTEGRITY** |
|  | **PASSWORDS AND SECURITY** |
|  | **PORTABLE COMPUTERS INCLUDING LAPTOPS AND TABLETS** |
|  | **UNAUTHORISED ACCESS** |
|  | **E-MAIL & ELECTRONIC MESSAGING** |
|  | **INTERNET POLICY** |
|  | **CATEGORIES OF INTERNET ACTIVITY** |
|  | **SOCIAL NETWORKING** |
|  | **TELEPHONE SYSTEM** |
|  | **MOBILE PHONES & OTHER MOBILE DEVICES** |
|  | **MONITORING** |
|  | **DISPOSAL OF I.T EQUIPMENT** |
|  | **MARKETING AND PR** |
|  | **USE OF PHOTOGRAPHS / VIDEO AND CONSENT** |
|  | **PHOTOGRAPHS OF STAFF** |
|  | **PHOTOGRAPHS OF SERVICE USERS** |
|  | **MARKETING PUBLICATIONS** |

6.0.1 Throughout this policy it is our aim:

* To provide reliable access to our company resources utilising a secure network, providing internal and external messaging systems and access to the internet without compromising security.
* To provide efficient fixed and mobile telephony, copying and printing.
* To provide support to users of these systems enabling their effective use.
* To maintain these systems in a timely and efficient manner.
  1. **ACCEPTABLE USE OF PHOENIX SUPPORT’ IT RESOURCES**

6.1.1 This document defines the policies to be followed by staff employed by Phoenix Support relating to computer usage, Internet, e-mail and computer security.

6.1.2 Phoenix Support’ IT resources comprise, without limitation, any computer (including laptops or tablets issued for off-site use), data network, and any telephone handset, switchboard or voice network provided or supported by the company, and includes interface with and use of public networks in conjunction with company IT facilities.

6.1.3 To develop a flexible and collaborative infrastructure the company may authorise the use of personal devices, such as laptops, Blackberries, Nokia Lumia Smart Phones, iPads and iPhones. Authority to use these devices is subject to agreeing to be bound by this policy and agreeing to connect your personal device to Phoenix Support’ systems, failure to comply with this policy will result in Disciplinary action.

6.1.4 The e-mail facility and access to the Internet and Intranet provided by Phoenix Support are intended to promote effective communication for the company and its clients on business matters. The company reserves the right to temporarily or permanently limit, withdraw or restrict use of, or access to any IT facilities.

6.1.5 Breach of this IT policy and/or misuse of company IT facilities may lead to disciplinary action being taken.

6.1.6 Nothing in this policy shall prohibit any of the company’s users from making a protected disclosure (often known as "whistle-blowing") under applicable law. All detected illegal activity or breaches of the ‘Computer Misuse Act 1990 (as amended)’ will be reported to the police authorities for further investigation.

* 1. **COMPUTER SYSTEMS POLICY**

6.2.1 All software used on any of the company’s computers must be approved in advance. Only personnel authorised may load software onto any of the company computers, connect any hardware or other equipment to any such computers or move or change any such computer equipment.

6.2.2 You must not make any copies of software except where this is expressly permitted by the copyright owner or as permitted by law. It is not permitted to use software for which Phoenix Support does not own a current user licence.

6.2.3 If you have a need for a particular software or hardware package, ask your manager, following consideration of your business case, we may arrange for the purchase.

**6.3 SYSTEM INTEGRITY**

6.3.1 It is the responsibility of each user to take all reasonable precautions to safeguard the security of any computer or device and the information contained upon it. This includes not allowing unauthorised users access to the machine.

6.3.2 An anti-virus software package is installed on each PC that we use or issue, however please do not rely on this software to protect your computer; you must adhere to the other precautions outlined in this policy.

6.3.3 Only removable storage media supplied by Phoenix Support should be used for data transmission. Phoenix Support allows access to all media via CareForIt, no storage of media is permitted without prior agreement from the General Manager.

**6.4 PASSWORDS AND SECURITY**

6.4.1 You are responsible for the security of your terminal, PC, iPad or laptop and for protecting any information or other data used and/or stored. You must not make copies of system configuration files for your own, unauthorised personal use or to provide to other people/users for unauthorised uses.

6.4.2 You must not allow your PC/terminal to be used by an unauthorised person.

6.4.3 You must keep your passwords confidential and change them regularly.

6.4.4 When leaving your PC/terminal unattended or on leaving the office, you must ensure that you log off the system or lock the screen to prevent unauthorised users using your terminal in your absence.

6.4.5 It is recommended that you change your password at least every 90 days, when changing your password it must meet the following requirements;

1. It must be a minimum of 7 characters long
2. Not contain more than 2 consecutive characters of your Username
3. It must contain 1uppercase characters (A through Z)
4. 1 lowercase characters (a through z)
5. 1 Base 10 digits (0 through 9)

**6.5 PORTABLE COMPUTERS INCLUDING LAPTOPS AND TABLETS**

6.5.1 Each individual is responsible for the portable device they use and must ensure that the correct procedures are followed, your laptop must be in your possession at all times.

6.5.2 Store portable devices in a secure area and out of sight when not in use. This includes your place of work, your home or any other location.

6.5.3 Do not display sensitive information in a public place where the screen could be overlooked.

6.5.4 No sensitive information should be held on the hard disk. You should ensure that all business data held on the hard disk is copied to the CareForIt system, all data storage is authorised for the CareForIt only.

6.5.5 All leavers should return the equipment to Head Office and not to their replacement, failure to do this may leave you liable to the cost of replacement

**6.6 UNAUTHORISED ACCESS**

6.6.1 To protect Phoenix Support’ systems and records and to preserve confidentiality, access to the company’s IT facilities are controlled.

6.6.2 If you have a legitimate business reason for wishing to access data or programs for which you do not have authorisation, you may only do so with the express authority of the General Manager or the owner of the data.

6.6.3 Use of programs, utilities and/or any other device designed to circumvent security measures, determine or identify passwords, breach conditional access systems, whether belonging to the company or to third parties, will be treated as a disciplinary matter

**6.7 E-MAIL & ELECTRONIC MESSAGING**

6.7.1 Phoenix Support provides several different internal and external electronic messaging systems for business use. These systems comprise of but are not limited to e-mail, messaging on the intranet and texting. For the purpose of this policy any reference to email also refers to all electronic communication methods provided by the company.

6.7.2 The e-mail and electronic messaging systems are the company’s property and the company reserves the right to monitor and to access any messages in the system.

6.7.3 Improper statements can give rise to legal action against you and/or Phoenix Support. Remember that advice given by e-mail may be relied upon and contracts may be created by e-mail.

6.7.4 All e-mail entering or leaving the company’s e-mail systems is stored and archived. This includes personal e-mails should you use the system for such a purpose. The deletion of a message or file will not fully eliminate it from the system

6.7.5 Always remember that e-mail messages, however personal, confidential or potentially damaging, may have to be disclosed in court proceedings if relevant to the issues.

6.7.6 Whilst it is accepted that you may need to send personal messages from time to time, you should respect the primary purpose of the e-mail system and keep personal use to a minimum. Use of the e-mail system for personal messages is subject to the company's right to monitor the system

**6.8 INTERNET POLICY**

6.8.1 We must adopt procedures which minimise the risk of using the Internet and follow good practice in the way individuals behave and the Internet sites that they visit.

6.8.2 You must not use the company’s IT facilities to access Internet sites which do not meet business requirements, and in particular any sites of an obscene, abusive, discriminatory or offensive nature.

6.8.3 Phoenix Support reserves the right to monitor the system for its legitimate business purposes, and by choosing to use the company’s IT facilities, you consent to the company monitoring all Internet sites you access

**6.9 CATEGORIES OF INTERNET ACTIVITY**

6.9.1 Internet activity (including e-mail) is generally grouped into four categories as follows:

(a) Business use: includes but is not limited to economic information, business news, etc.

(b) Non-business but acceptable use: news, weather, responsible brief personal use

(c) Misuse: this includes excessive time, large downloads, games, chat rooms

(d) Inappropriate use: this includes pornographic or adult-orientated websites or e-mails

6.9.2 Disciplinary action will be taken against any employee where usage falls into the categories listed in (c) and (d) above.

6.9.3 Where material is obtained from the Internet, ensure that any copyright restrictions are obeyed and that virus protection procedures are followed.

**6.10** **SOCIAL NETWORKING**

6.10.1 The growth of social networking particularly Twitter, Facebook and Instagram has created a platform to use as a method of identifying individuals to use for personal gain of information on clients or ourselves. Therefore when using these types of social networking sites users should not;

* befriend or accept friend requests from service users on any social media platform

• mention or detail clients or client information directly or indirectly,

• access these sites for any periods during working hours

• create social groups around Phoenix Support’ name.

6.10.2 Users of these sites are advised to secure their profile so that it is not accessed without the knowledge.

**6.11 TELEPHONE SYSTEM**

6.11.1 You are reminded that the use of the telephone for personal calls is prohibited unless in an emergency situation, and is closely monitored.

6.11.2 Anyone who makes persistent use of the telephone for personal calls will be asked to provide an explanation.

6.11.3 Phoenix Support reserves the right, if appropriate, to claim reimbursement for all personal calls made.

**6.12 MOBILE PHONES & OTHER MOBILE DEVICES**

6.12.1 Your mobile device contains confidential information. User should ensure they activate any security measures such as the setting of PIN numbers and passwords as are available on the device.

6.12.2 Do not leave yourself open to the theft of your mobile device, exercise caution at all times and remain aware of the surroundings.

6.12.3 Phoenix Support reserves the right to pass on to you any charges incurred by the company for unauthorised use, including data or internet usage.

6.12.4 The mobile device handset, charger and any other accessories remain the property of Phoenix Support. The person to whom it has been issued is responsible for its correct use and safekeeping. Any loss of a mobile handset shall be reported immediately to Head Office, and the police. Where the loss is attributable to the lack of care on the part of the user, he/she may be responsible for any costs incurred.

6.12.5 The use of mobile devices whilst driving is banned. Anyone driving a vehicle on business must not make or receive any calls during the journey. You must be in proper control of your vehicle at all times. Any lack of concentration or momentary inattention may result in you being prosecuted.

6.12.6 Confidential information must not be disclosed over a mobile device as it may be overheard by people in the immediate vicinity.

6.12.7 For personal mobile devices, by agreeing to connect your mobile device to the company’s information systems you agree to:

• Enforce a security PIN or password on the device.

• Deliver the device to Phoenix Support for physical audit as and when requested

• To comply with Phoenix Support’ internet and security policies at all times.

**6.13 MONITORING**

6.13.1 Phoenix Support reserves the right to audit, monitor or record any communications or other component of the IT facilities and systems, for compliance with this policy;

* to establish the existence of facts;
* to ascertain or demonstrate standards which are or ought to be achieved
* to prevent, investigate or detect crime and disciplinary offences;
* to investigate or detect unauthorised or illicit use of the IT system;
* to determine whether communications are relevant to the business or are personal

6.13.2 A non-exhaustive list of examples of monitoring carried out by Phoenix Support are as follows:

* Where CCTV is present, employees must be aware they may be captured on this and footage could be used accessed for any investigation
* opening employees' e-mails or listening to their voice-mails during any form of investigation
* examining logs of websites visited, and other internet history
* keeping records of telephone calls made to be charged against or used in any investigation
* systematically checking logs of telephone numbers called to detect use of premium calls

**6.14 DISPOSAL OF I.T EQUIPMENT**

6.14.1 Phoenix Support takes it’s responsibility to the environment and the social implications of doing business very seriously, therefore no electrical, electronic or IT related waste should be destroyed or disposed of without first gaining approval from the General Manager.

6.14.2 Procedures are in place to collect and destroy or redistribute this type of waste to ensure Phoenix Support complies with the Waste of Electrical and Electronic equipment (WEEE) and GDPR2018 Regulations.

**6.15 MARKETING AND PR**

6.15.1 The aim of Phoenix Support marketing strategy is in communicating with the press on all good news stories and marketing activity. (All negative press is communicated and handled by the General Manager with support from the Senior Management team.

6.15.2 To offer support and understanding to staff on marketing and activity that takes place throughout the organisation.

6.15.3 To manage and enhance a consistent image of the organisation in the public domain and online. To offer a consistent brand message and style by the use of a centralised system of production, design and print work.

6.15.4 To support all corporate departments with internal communications, and support the business units with business growth and recruitment.

6.15.5 To advise and facilitate public promotions and exhibitions, writing and producing the corporate newsletter and Annual Reviews. Managing all social media and online activity.

**6.16 USE OF PHOTOGRAPHS / VIDEO AND CONSENT**

6.16.1 Phoenix Support will identify a variety of publications and marketing material, including the use of online marketing tools. Where possible Phoenix Support endeavours to use positive images of staff and service users. The privacy and dignity of service users must be protected at all times.

6.16.2 No photographs should be used for publication without the consent of the person in the image or footage

**6.17 PHOTOGRAPHS OF STAFF**

6.17.1 During any period of employment, photographs / video footage may be taken of staff members as they undertake the duties of their role, participate in training or corporate/local events, attend conferences/seminars, etc. Phoenix Support reserves the right to use such photographs / video footage in publicity, social media, advertising and training materials both internally and externally. At all times copyright of such images will remain the property of Phoenix Support.

**6.18 PHOTOGRAPHS OF SERVICE USERS**

6.18.1 When taking photographs / filming video footage, the photographer/staff member must first obtain the permission of the service user.

6.18.2 Each service user will be asked to complete and sign a Model Release Formagreeing that any photographs / video footage in which they feature during the time they are receiving support may be used for publications, social media, press releases, advertisements and/or use on the corporate website.

6.18.3 The staff member should ensure that the content of the Model Release Form is explained clearly to, and is fully understood by, the service user. If consent has not been given and a model release form has not been filled in and signed for a service user, this must be logged within the service users file. The staff member must also send the service user’s details to the marketing department to ensure photographs and video footage do not include this individual.

6.18.4 If a service user is aged under 18 years, permission to use photographs / video footage must be sought from the service user’s parent or guardian.

6.18.5 Any agreement entered into with a professional photographer, videographer, printer/designer and/or other third party should clearly state that at all times copyright of the images obtained remains the property of Phoenix Support.

6.18.6 If a service user subsequently requests that an image is not utilised this request should be forwarded to Head Office who will ensure that the image is withdrawn. However, it should be explained to the service user that it is not possible for the photographic image to be withdrawn from existing publications that may be in circulation.

**6.19 MARKETING PUBLICATIONS**

6.19.1 These are to be designed as required and will be circulated to an agreed audience, any marketing using the Phoenix Support name or logo, must be authorised by the General Manager or member of the senior Management team.