Acceptable Use Policy

Version number: 1.0

Publish date: 16-05-2018

Document control	
Prepared by	Mike Moore, Managing Director
Authorised by	Upper Management
Physical Copy location(s)	Operations Folder
Source Copy Location(s)	Dropbox - GDPR123\Documents\Final Documents
Published Copy Location(s)	www.Dephoto.biz\GDPR
Other Referenced Documents	Information Security Policy, Data Protection Policy, Monitoring Policy, Access Control Policy, Device Management Policy, Password Policy, Confidential Information Policy, Non-Discrimination and Anti-Harassment Policy
Related Material	
Acknowledgements	GDPR123
Distribution	Upper Management, Franchise Owners, All Staff

Version Control				
Title	Acceptable Use Policy			
Description	To ensure that all complaints about data protection and information security get handled in the correct manner, ensuring there are records of what is submitted and how the complaint is handled.			
Created by	Mike Moore			
Date Created	16-05-2018			
Maintained by	Upper Management			
Version Number	Modified By	Modifications Made	Date Modified	Status
1.0	Mike Moore	First creation	16-05-2018	Published

Unit 19 Lambs Business Park, South Godstone, RH9 8LJ | www.DEphoto.biz | 01342 894519
DE Photo (Franchising) Ltd. | Company Reg No. 5160591 | ICO Reg No. Z2569824

Contents

Unit 19 Lambs Business Park, South Godstone, RH9 8LJ | www.DEphoto.biz | 01342 894519
DE Photo (Franchising) Ltd. | Company Reg No. 5160591 | ICO Reg No. Z2569824

Purpose

This policy is a supporting policy of the Information Security Policy, so the purpose of this policy is the same, to secure information. DE Photo (Franchising) Ltd (referred to as the company here after) takes information security very seriously. To make sure that information security is not compromised by system misuse, this policy outlines the acceptable use of computer equipment at the company. These rules are in place to protect the employee and the company. Inappropriate use exposes the company to risks including virus attacks, compromise of network systems and services, and legal issues.

Scope

This policy applies to the use of information, electronic and computing devices, and network resources to conduct the company's operations or interactions with internal networks and business systems, whether owned or leased by the company, the employee, or a third party. All employees, franchisees, contractors, consultants, temporary, and other workers at the company and its subsidiaries are responsible for exercising good judgment regarding appropriate use of information, electronic devices, and network resources in accordance with the company's policies and standards, and local laws and regulations. Exceptions to this policy are documented in this policy.

This policy applies to employees, franchisees, contractors, consultants, temporaries, and other workers at the company, including all personnel affiliated with third parties. This policy applies to all equipment that is owned or leased by the company.

Definitions and terms

Blogging – An online journal that is used convey opinions and news.

Honeypot – A device that is designed to encourage attack.

Honey-net – A network that is designed to encourage attack.

Proprietary Information – Information related to the running of the company that if lost or misused could cause damage or monetary loss. Examples include but is not limited to propriety information including code for programs, business strategy plans or automation algorithms.

Spam – Unsolicited messages sent in bulk

Unit 19 Lambs Business Park, South Godstone, RH9 8LJ | www.DEphoto.biz | 01342 894519
DE Photo (Franchising) Ltd. | Company Reg No. 5160591 | ICO Reg No. Z2569824

Policy

General Use and Ownership

The company's proprietary information whether stored on electronic and computing devices owned or leased by the company, the employee or a third party, remains the sole property of the company. All employees, contractors or related third parties must ensure through legal or technical means that proprietary information is protected in accordance with the Information Security Policy and the Data Protection Policy.

All employees, contractors or related third parties have a responsibility to promptly report the theft, loss or unauthorised disclosure of the company proprietary information using the Reporting Information Security Weaknesses and Events Procedure.

For security and network maintenance purposes, authorised individuals within the company may monitor equipment, systems and network traffic at any time in accordance with the Monitoring Policy.

the company reserves the right to audit networks and systems on a periodic basis to ensure compliance with this policy.

Security and Proprietary Information

All mobile and computing devices that connect to the internal network must comply with the company's Access Control Policy and the Device Management Policy.

System level and user level passwords must comply with the Password Policy. Providing access to another individual, either deliberately or through failure to secure its access, is prohibited.

All computing devices must be secured with a password-protected screensaver. All employees, contractors or related third parties must lock the screen or log off when the device is unattended.

Postings by employees from the company email addresses to newsgroups should contain a disclaimer stating that the opinions expressed are strictly their own and not necessarily those of the company, unless posting is in the course of business duties and authorised by Head Office or marketing duties.

Employees must use extreme caution when opening e-mail attachments received from unknown senders, which may contain malware.

Unit 19 Lambs Business Park, South Godstone, RH9 8LJ | www.DEphoto.biz | 01342 894519
DE Photo (Franchising) Ltd. | Company Reg No. 5160591 | ICO Reg No. Z2569824

Unacceptable Use

The following activities are, in general, prohibited. Employees and Franchisees may be exempted from these restrictions during the course of their legitimate job responsibilities (e.g. systems administration staff may have a need to disable the network access of a host if that host is disrupting production services).

Under no circumstances is an employee or franchisee of the company authorised to engage in any activity that is illegal whilst using the company resources or when on company premises.

The lists below are by no means exhaustive, but attempt to provide a framework for activities which fall into the category of unacceptable use.

System and Network Activities

The following activities are strictly prohibited, with no exceptions:

1. Violations of the rights of any person or company protected by copyright, trade secret, patent or other intellectual property, or similar laws or regulations, including, but not limited to, the installation or distribution of unlicensed or illegal software or software products that do not contain an appropriate license or rights for use by the company.
2. Unauthorised copying of copyrighted material including, but not limited to, digitisation and distribution of photographs, books or other copyrighted sources and the installation of any copyrighted software for which the company or the end user does not have a sufficient active license is strictly prohibited.
3. Accessing data, a server or an account for any purpose other than conducting the company business, even if all employees, franchisees, contractors or related third parties have authorised access, is prohibited.
4. Introduction of malicious programs into the network or server (e.g. viruses, worms, Trojan horses, e-mail bombs, etc.).
5. Revealing any authorisation/authentication information such as passwords, pins codes, ID or encryption keys to others or allowing use of an account by unauthorised personnel. This includes family and other household members when work is being done at home.
6. Using a the company computing asset to actively engage in procuring or transmitting material that is in violation of sexual harassment or hostile workplace laws in the UK.
7. Making fraudulent offers of products, items, or services originating from any company account.
8. Effecting security breaches or disruptions of network communication. Security breaches include, but are not limited to, accessing data of which the employee or franchisee is not an intended recipient or logging into a server or account that the employee or franchisee is not expressly authorised to access, unless these duties are within the scope of regular duties. For purposes of this section, "disruption" includes, but is not limited to, network sniffing, pinged floods, packet spoofing, denial of service, and forged routing information for malicious purposes.

Unit 19 Lambs Business Park, South Godstone, RH9 8LJ | www.DEphoto.biz | 01342 894519
DE Photo (Franchising) Ltd. | Company Reg No. 5160591 | ICO Reg No. Z2569824

9. Port scanning or security scanning is expressly prohibited unless prior notification to product owners and permission is obtained.
10. Executing any form of network monitoring which will intercept data not intended for the employee's host, unless this activity is a part of the employee's normal job/duty.
11. Circumventing user authentication or security of any host, network or account.
12. Introducing honeypots, honey-nets, or similar technology on the company network without explicit consent and permission is granted and documented by the information security department.
13. Interfering with or denying service to any user other than the employee's host (for example, denial of service attack).
14. Using any program/script/command, or sending messages of any kind, with the intent to interfere with, or disable, a user's workflow or productivity, via any means, locally or via the Internet/Intranet/Extranet.

Email and Communication Activities

1. When using company resources to access and use the Internet, users must realise they represent the company.
2. Whenever employees or franchisees state an affiliation to the company, they must also clearly indicate that "the opinions expressed are my own and not necessarily those of the company". Questions may be addressed to the IT Department or passed through the reporting line.
3. Sending unsolicited email messages, including the sending of "junk mail" or other advertising material to individuals who did not specifically request such material (email spam) and where consent is not valid or provable.
4. Any form of harassment via email, telephone or paging, whether through language, frequency, or size of messages.
5. Unauthorised use, or forging, of email header information.
6. Solicitation of email for any other email address, other than that of the poster's account, with the intent to harass or to collect replies.
7. Creating or forwarding "chain letters".
8. Use of unsolicited email originating from within the company's networks of other Internet/Intranet/Extranet service providers on behalf of, or to advertise, any service hosted by the company or connected via the company's network.
9. Posting the same or similar non-business-related messages to large numbers newsgroups (newsgroup spam).

Unit 19 Lambs Business Park, South Godstone, RH9 8LJ | www.DEphoto.biz | 01342 894519
DE Photo (Franchising) Ltd. | Company Reg No. 5160591 | ICO Reg No. Z2569824

Blogging and Social Media

1. Blogging by employees or franchisees, whether using the company's property and systems or personal computer systems, is also subject to the terms and restrictions set forth in this Policy.
2. Limited and occasional use of the company's systems to engage in blogging is acceptable, provided that it is done in a professional and responsible manner, does not otherwise violate the company's policy, is not detrimental to the company's best interests, and does not interfere with an employee's or franchisee's regular work duties. Blogging from the company's systems is also subject to monitoring in accordance with the Monitoring Policy.
3. The company's Confidential Information Policy also applies to blogging. As such, employees and franchisees are prohibited from revealing any the company confidential or proprietary information, trade secrets or any other material covered by the company's Confidential Information Policy when engaged in blogging.
4. Employees and franchisees shall not engage in any blogging that may harm or tarnish the image, reputation and/or goodwill of the company and/or any of its employees or franchisees. Employees and franchisees are also prohibited from making any discriminatory, disparaging, defamatory or harassing comments when blogging or otherwise engaging in any conduct prohibited by the company's Non-Discrimination and Anti-Harassment Policy.
5. Employees and franchisees may also not attribute personal statements, opinions or beliefs to the company when engaged in blogging. If an employee is expressing his or her beliefs and/or opinions in blogs, the employee may not, expressly or implicitly, represent themselves as an employee or representative of the company. Employees and franchisees assume any and all risk associated with blogging.
6. Apart from following all laws pertaining to the handling and disclosure of copyrighted or export controlled materials, The company's trademarks, logos and any other the company intellectual property may not be used in connection with any blogging activity outside of authorised company marketing communications.

Unit 19 Lambs Business Park, South Godstone, RH9 8LJ | www.DEphoto.biz | 01342 894519
DE Photo (Franchising) Ltd. | Company Reg No. 5160591 | ICO Reg No. Z2569824

Compliance

Compliance Measurement

Compliance to this policy will be audited through various methods, including but not limited to, periodic training, video monitoring, business reports, internal and external audits, and feedback to the policy owner.

Exceptions

Any exception to the policy must be approved by the business process owners in advance.

Non-compliance

Compliance with this policy is not optional, any employees or franchisees that are found to have violated this policy will be subject to the disciplinary terms detailed in the Data Protection Policy in line with the severity of the offence and the damages caused.

Contractors or related third parties that are found to have violated this policy will be liable for damages as laid out in the contract terms and may be subject to legal actions.

Management and Review

This policy should be reviewed as scheduled once annually unless performance indicators, changes to legislation or the organisation necessitate it.

Last Review Date: 16/05/2018

Next Review Date: 16/05/2019

Unit 19 Lambs Business Park, South Godstone, RH9 8LJ | www.DEphoto.biz | 01342 894519
DE Photo (Franchising) Ltd. | Company Reg No. 5160591 | ICO Reg No. Z2569824