Clean Desk 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
Related Material	
Acknowledgements	GDPR123
Distribution	Upper Management, Franchise Owners, All Staff

Version Control				
Title	Clean Desk Policy			
Description	To make sure that there is no information left in or around work areas, this policy establishes the minimum requirements for maintaining a "clean desk".			
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) take information security very seriously. In order to make sure that there is no information left in or around work areas, this policy establishes the minimum requirements for maintaining a "clean desk". This policy will mitigate the risk of information disclosure by removing information from work areas.

Scope

This policy applies to any area where employees, franchisees, affiliates, temporary employees and contractors are working or using the company's systems.

Policy

Employees are required to ensure that all sensitive/confidential information in hardcopy or electronic form is secure in their work area at the end of the day or if they are expected to be gone for an extended period.

Computer workstations must be locked when a user leaves their workspace unattended.

Any restricted or sensitive information must be removed from the desk and locked away securely when the desk is unoccupied and at the end of the work day.

File cabinets containing restricted or sensitive information must be kept closed and locked when not in use or when not attended.

Keys/access control cards/fobs used for access to restricted or sensitive information must not be left at an unattended desk.

Laptops must be either locked with a locking cable or locked away in a drawer or store room.

Passwords, security codes, encryption keys or other authorisation / authentication information may not be left on sticky notes posted on or under a computer, nor may they be left written down in an accessible location.

Printouts containing restricted or sensitive information should be immediately removed from the printer.

Upon disposal, restricted and/or sensitive documents should be shredded using a crosscut shredder of DIN 66399-3 standard or higher or placed in locked confidential waste bins.

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

Whiteboards containing restricted and/or sensitive information should be erased when not in use.

All portable devices such as phones, tablets, laptops and any other portable device that may or may not contain sensitive company information should be stored in a locked cupboard or store room when not in use.

All devices of this type should be logged and locations of such devices should be known at all times.

Treat mass storage devices such as CD-ROMs, DVDs or USB drives as sensitive and secure them in a locked drawer or store room.

All printers, scanners/photocopiers and fax machines should be cleared of papers as soon as they are used; this helps ensure that sensitive documents are not left in printer trays or on scanners/photocopiers for the wrong person to pick up.

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. Compliance staff may perform spot checks on work areas.

Exceptions

Any exception to the policy must be approved by the information security department in advance.

Non-Compliance

Compliance with this policy is not optional, any employees 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 action.

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