Removable Media 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	Data Protection Policy
Related Material	
Acknowledgements	GDPR123
Distribution	Upper Management, Franchise Owners, All Staff

Version Control				
Title	Removable Media Policy			
Description	In order for data to be safely stored and transferred on removable media, this policy establishes the principles and working practices that are to be followed by all people that fall under the scope.			
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 is the same, to secure information. DE Photo (Franchising) Ltd (referred to as the company here after) take information security very seriously. In order for data to be safely stored and transferred on removable media, this policy establishes the principles and working practices that are to be followed by all people that fall under the scope.

This policy aims to ensure that the use of removable media devices is controlled in order to:

- Enable the correct data to be made available where it is required.
- Maintain the integrity of the data.
- Prevent unintended or deliberate consequences to the stability of the company's computer network.
- Comply with any legislation, policies or good practice requirements.
- Maintain high standards of care in ensuring the security of protected and restricted information.
- Prohibit the disclosure of information as may be necessary by law.

Scope

This policy applies to all staff, employees, franchisees, contractual third parties and visitors of the company who have access to company information, information systems or IT equipment and intends to store any information on removable media devices.]

Definitions

This policy should be adhered to at all times, but specifically whenever any user intends to store any information on removable media devices.

Removable media devices include, but are not restricted to the following:

- Optical discs (CDs, DVDs, Blu-rays)
- Hard Drives
- USB Memory Sticks (also known as pen drives or flash drives)

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

Risks

The company recognises that there are risks associated with users accessing and handling information. Securing data is of paramount importance – particularly in relation to the company's need to protect data in line with the requirements of the GDPR.

This policy aims to mitigate the following risks:

- Breach of data as a consequence of loss, theft or careless use of removable media devices.
- Contamination of networks or equipment through the introduction of viruses through the transfer of data from one form of IT equipment to another.
- Potential sanctions against company employees imposed by the Information Commissioner's Office as a result of information loss or misuse.
- Potential legal action against the company as a result of information loss or misuse.
- Reputational damage as a result of information loss or misuse.

Non-compliance with this policy could have a significant effect on the efficient operation of the company and may result in financial loss and an inability to provide necessary services to customers.

Policy

Restricted Access to Removable Media

The use of removable media devices will only be approved if a valid business case for its use is developed and all necessary risk assessments have been carried out and documented.

There are large risks associated with the use of removable media, and therefore clear business benefits that outweigh the risks must be demonstrated before approval is given.

Requests for access to, and use of, removable media devices must be made to the information security dept. Approval for their use must be given and documented.

Should access to, and use of, removable media devices be approved, the following sections apply and must be adhered to at all times.

Procurement of Removable Media

All removable media devices, equipment and software must be purchased or recommended by the IT administration dept. Non-company owned removable media devices must not be used.

The only equipment and media that should be used to connect to the company equipment or the internal network is media that has been recommended by the company and approved by the information security dept.

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

Security of Data

Data that is only held in one place and in one format is at much higher risk of becoming unavailable or corrupted through loss, destruction or malfunction of equipment than data which is frequently backed up. Removable media should not be the only place where data obtained is held. Copies of any data stored on removable media must also remain at the original location and potentially backed up on a regular basis until the data is successfully transferred to the destination system.

In order to minimise physical risk, loss, theft or electrical corruption, all storage media must be stored in an appropriately secure and safe environment. All media should be asset registered and logged in and out so all removable media devices should be accounted for and locations should be known.

Each user is responsible for the appropriate use and security of data and for not allowing removable media devices, and the information stored on these devices, to be compromised in any way whilst in their care or under their control.

All data stored on removable media devices (with the exception of customer purchased USB Sticks supplied by the company) must be encrypted using the standards defined in the Encryption Policy.

Incident Management

It is the duty of all users to immediately report any actual or suspected breaches in information security.

Any misuse or irresponsible actions that affect business data, or any loss of data, should be reported as a security incident to the information security dept. or management.

Third Party Access

No third party (external contractors, partners, agents, the public or non-employee parties) may receive data or extract information from the company's internal network, information stores or IT equipment without explicit agreement from the information security dept.

Should third parties be allowed access to information then all the considerations of this policy apply to their storing and transferring of the data and should be stated as such in a legally binding and enforceable agreement such as a contract.

Preventing Information Security Incidents

Damaged or faulty removable media devices must not be used. It is the duty of all users to contact the IT administration dept. should removable media be damaged.

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

Virus and malware checking software approved by the information security dept. must be operational on both the machine from which the data is taken and the machine on to which the data is to be loaded.

The data must be scanned by approved virus checking software products, before the media is loaded on to the receiving machine.

Whilst in transit or storage the data held on any removable media devices must be given appropriate security according to the type of data and its sensitivity. Encryption and password control must be applied to the data files.

Disposing of Removable Media Devices

Removable media devices that are no longer required, or have become damaged, must be disposed of securely to avoid data leakage. Any previous contents of any reusable media that are to be reused, within the company, must be erased. This must be a thorough removal of all data from the media to avoid potential data leakage using specialist software and tools. All removable media devices that are no longer required, or have become damaged, must be marked for secure disposal following the Disposals Procedure.

User Responsibility

All considerations of this policy must be adhered to at all times when using all types of removable media devices.

However, special attention must be paid to the following when using USB memory sticks (also known as pen drives or flash drives), recordable CDs, DVDs and diskettes:

- Any removable media device used must be purchased or recommended by the IT administration dept.
- Any removable media device that has not been supplied by IT must not be used.
- All data stored on removable media devices must be encrypted.
- Virus and malware checking software must be used when the removable media device is connected to a machine.
- Only data that is authorised and necessary to be transferred should be saved on to the removable media device.
- Removable media devices must not to be used for archiving or storing records as an alternative to other storage equipment.
- Special care must be taken to physically protect the removable media device and stored data from loss, theft or damage.
- Anyone using removable media devices to transfer data must consider the most appropriate way to transport the device and be able to demonstrate that they took reasonable care to avoid damage or loss.

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 in advance and listed below.

- Customer purchased USB Sticks supplied by the company

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 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