# Remote & Mobile Working 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 | Access Control Policy, Boundary Device Protection Policy, Encryption Policy, Disposals Procedure, Acceptable Use Policy, Data Protection Policy |
| Related Material | |
| Acknowledgements | GDPR123 |
| Distribution | Upper Management, Franchise Owners, All Staff |

| Version Control | | | | |
|---|---|---|---|---|
| Title | Remote & Mobile Working Policy | | | |
| Description | Ensuring security to mitigate risks from all personnel that use or remotely access the company data records. | | | |
| 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

## Introduction

Remote working presents significant risks for the security and integrity of data records and information DE Photo (Franchising) Ltd (referred to as the company here after) controls. This policy focuses on ensuring security in three key areas to mitigate these risks:

- Securing entry to the company systems from unauthorised outside connections.
- Securing data in transit when information is accessed remotely.
- Securing data on the remote device once it is accessed.

## Scope

This guideline applies to employees, franchisees, contractors, consultants and other workers using equipment owned by or accessing information held by the company. This policy applies to all personnel that use or remotely access the company data records. It applies to all staff and franchisees working from home or not from the company fixed site.

## Definitions

GDPR – Regulation (EU) 2016/679 the General Data Protection Regulation, legislation that governs data protection in the EU

IP address – A sequence of numbers used in identifying devices on the internet

Unique User ID – Method of identifying users for example, a username

VPN – Virtual private network, a method of connecting a device to a local network over the internet using encrypted tunnelling protocols.


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

## Requesting access

By default no one is to have any form of remote access setup. To gain remote access an official request needs to be made to the information security department who will consider the request by performing the necessary risk assessments.

The risk assessment should consider the following:

- The sensitivity of the information to be processed.
- The security of the equipment to be used.
- The suitability of the proposed location for remote working.
- The most secure way of working in the context.

Should the request be approved the level of access granted must follow the principle of least privilege and the standards laid out in the Access Control Policy. A written remote working agreement should be issued to the entity that requested access and should regulate how the entity works remotely and include provisions for secure access.

The information security dept. must ensure that all parties working remotely are aware of their responsibilities under the GDPR and the policies and procedures of the company.

To ensure the security of sensitive personal data, remote access to systems that contain personal data will not be granted and requests to access these systems will always be denied. Sensitive personal data includes but is not limited to:

- Racial or ethnic origins
- Political opinions
- Religious beliefs
- Membership of a trade union
- Physical or mental health
- Sexual life
- Criminal records


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

## Providing access

Any connection setup for remote access should comply with the Boundary Device Protection Policy. All connections must be encrypted according to the Encryption Policy and use a strong authentication mechanism.

The systems allowing connection must log the IP address and unique user ID and where possible record all actions taken. Failed attempts to gain access must also be logged. These logs should be regularly reviewed by the information security dept.

## Securing remote and mobile workers

All remote and mobile workers should take reasonable precautions to protect against the loss or interference of any company information, data, software, systems, networks or customer records.

Such precautions should include but are not limited to:

- Taking appropriate measures to physically secure office equipment and work related information from theft or accidental loss or damage.
- Ensuring that office equipment (e.g. laptop) and hard copy documents are not left unattended where this might constitute a risk.
- Ensuring that casual passers-by or other unauthorised persons cannot read information where this might constitute a risk (e.g. when entering passwords, accessing sensitive personal data).
- Ensuring that office equipment and hard copy documents are not accessible to unauthorised users (such as family, friends, etc.).
- Making sure office equipment and hard copy documents left unattended in a parked vehicle are locked away in a secure out of sight location, for example the glove box.
- Working directly from the company's network via a secure VPN connection and not using shared unprotected Wi-Fi.
- Save any electronic documents produced at home on to the company's network via a secure VPN connection and not using shared unprotected Wi-Fi.
- If authorised to take documents out of the working area, ensure that they are copies and not the originals.
- Return copies of documents to the office to ensure that they are disposed of according to the Disposals Procedure.


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

Remote and mobile workers are expected to follow the Acceptable Use Policy which includes not doing any of the following:

- Downloading, installing or using unauthorised or illegal software programs.
- Storing, using, coping or circulating inappropriate materials (e.g. pornographic, sexually explicit, or racially offensive material) on any device.
- Using your unauthorised devices to perform work-related activities.
- Using personal email accounts for work-related business.
- Unauthorised processing of sensitive personal information.

## Equipment

Remote and mobile workers provided with company equipment to work remotely must only use this for legitimate work-related purposes.

The equipment provided may only be modified or replaced by the IT administration dept. or a third party company authorised to do so by the information security dept.

Remote and mobile workers are responsible for the safekeeping and protection of company equipment issued to them. They are also responsible for preventing unauthorised persons from accessing them.

If company equipment is lost or stolen, the authorities and the information security dept. should be notified immediately.

Information security incidents (e.g. virus infections) on company equipment or approved remote and mobile working equipment should be reported as stated in the “Reporting Information Security Weaknesses and Events Procedure” to the information security dept.

The damage, loss or theft of any work-related information while working remotely should be reported to the information security dept. immediately; where damage, loss or theft of sensitive personal information is possible, this must be reported immediately to enable a data protection breach to be dealt with according to the Data Breach Response Plan.


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

## Monitoring and 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 information security dept.

## Exceptions

Any exception to the policy must be approved by the information security dept. 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