BIOMETRIC DATA POLICY

Introduction

The reason for this policy is to enable the use of fingerprint scanning software at Company sites to meet the following objectives:

- Provide greater security of the site in respect of authorised employees, workers and contractors who access the site.
- Allow training records to be logged against employees, workers and contractors in order that site managers can be sure that individuals have completed the required training before entry to work on site.
- Allow authorised employees, workers and contractors from the Company to access another Company site using their biometric data.
- Maintain records of attendance at each site.

A policy is required because of the data protection issues raised by fingerprint scanning. Any personal data that is stored falls under the Data Protection Act 2018 and the General Data Protection Regulation 2018 (GDPR). As biometric data (i.e. fingerprints) is sensitive personal data, it is important to have a record of the facts about the system and a policy on its use.

Factual Background

There are data protection issues surrounding the safeguarding of 'high level' biometric data (e.g. fingerprint images). The Company system does not collect and store fingerprint images. The scanner only takes part of the fingerprint and creates a unique code which is stored in a password protected database on the site computer, which we refer to as 'Security Access Data'.

It may be possible to make a machine that 'reverse engineers' the Security Access Data to re-create the sample points, but this would not give a full or detailed fingerprint and the effort / benefit of doing so would make it an unlikely target for compromising data.

Data Protection Act

This policy has been prepared with regard to the Data Protection Act 2018 and the General Data Protection Regulation (GDPR) 2018. This policy should also be read in conjunction with the Data Protection Policy Statement.

For the purposes of the Data Protection Act:

- The employee, worker or contractor is the 'Data Subject'. The data subject is informed and consulted about the use of their personal data.
- The 'data controller' is the Company.
- The 'data processor' is the employee of the Company responsible for the biometric data software and its implementation across the Company and any site managers or Company IT personnel who have also been given access to process the biometric Company data.

Awareness

All employees, workers and contractors joining and working for the Company, who will need to provide biometric data for Company site access, will have access this Biometric Data Policy and the Data Protection Policy Statement.

- The Data Protection Policy Statement explains:
- What personal information we collect
- How personal information is collected

- Why we collect personal information
- How we use personal information
- Who we may share information with
- Where information is processed
- How we protect information
- How long we use information for
- How we approach automated decision-making
- Rights in connection with personal information

Reason for collecting Biometric data

The biometric fingerprint data provided by individuals will be used to ensure their security and safety whilst on the site and to prevent any unauthorised access. It will also be used to monitor working hours for compliance with the Working Time Regulations (SI 1998/1833)

Length of time the data is stored for

Biometric personal data will be retained by the Company for as long as it fulfils its specific purpose, that being site access, to access details of training received by an individual and to provide records of attendance on a site.

There is no reason to retain biometric data after a data subject has left the employment of the Company or after the contractual relationship is at an end, if the data subject is a self-employed contractor, and the project has been completed for twelve months.

Protection of Data

The personal biometric data is protected from unauthorised access. This information can only be accessed from the Administrator account, by authorised members of staff.

The biometric data stored will not allow an individual to recreate a fingerprint.

Review

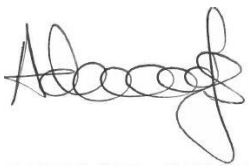
This policy will be reviewed annually, or where there are changes in legislation that affect the policy.

Disciplinary Action

The Company has systems in place to monitor the system and will act immediately if there is any risk that this policy may be breached or not followed.

Signed: 

Francis Shiner – Managing Director

Signed: 

Adam Knaggs – Director

Signed: 

Martin Lowndes – Director

Signed: 

Craig Millar – Director

Signed: 

Gary Wykes - Director

Date: **January 2019**

Next Review Date: **January 2020**