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 1998. 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

The Data Protection Act 1998 includes eight data protection principles with which data controllers must comply. The first, second, fifth and seventh principles are the most relevant to this issue.

- The first principle requires that personal data is processed fairly and lawfully. Fairness requires that the Company informs employees, contractors and workers who will be required to supply biometric data the purposes for the collection of this data so that they understand the purpose for which their personal data is being processed.
- The second principle requires that personal data is obtained for one or more specified and lawful purposes and not further processed in any manner incompatible with that purpose or those purposes. Biometric data should therefore not be used for any purpose not directly related to that for which it was collected.
- The fifth principle requires that personal data is not kept for longer than it is needed for its specified purpose. Biometric data should therefore be destroyed when an individual has left the Company and the requirement for records of attendance on a project ends.
- The seventh principle requires that the appropriate security is in place to safeguard personal data from unauthorised processing and accidental loss, destruction or damage.

This policy has been prepared with regard to the Data Protection Act 1998 and Information Commissioner's Office guidance. This policy should also be read in conjunction with the Data Protection Policy.

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 password access to process the biometric Company data.

The Data Protection Act sets out 'sensitive personal data' as covering data such as personal medical information of a data subject. Guidance for the General Data Protection Regulations, which are due to become law in May 2018, include 'special categories of personal data' including the use of genetic and biometric data. This policy is mindful of the changes to Data Protection regulations.

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 to Biometric Data Use Policy as well as an explanation of the following information:

- The nature of the biometric fingerprint-based system and what personal data is stored by the system.
- The member(s) of staff who are responsible for implementing the biometric fingerprint-based system providing and managing and updating the software.
- Those members of staff who directly line manage the employee, worker or contractor and who will have access to the biometric data for secure access purposes and for checking training has been received.
- The member(s) of staff responsible for deleting data subject biometric records or amending this data.

Consent

Individuals who will be asked to provide biometric fingerprint data will be asked to sign a separate consent form prior to obtaining this data.

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. (Data Protection Act fifth principle).

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 (Data Protection Act seventh principle). This information can only be accessed from the Administrator account, by those members of staff who are specified above. As with all access to personal data, the username and password for this account should be restricted on a need-to-know basis and is changed on a regular basis. The biometric data stored will not allow an individual to recreate a fingerprint as explained earlier in this policy.

Review

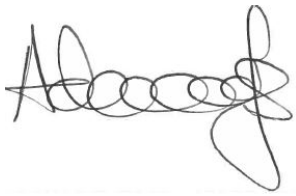
HR has a responsibility to ensure that this policy is reviewed every two years, or where there are changes in legislation that affect this policy.

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: **September 2017**

Next Review Date: **September 2018**